



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

---

1999-09-01

A revitalized information assurance training  
approach and information assurance best  
practice rule set

Pappas, James A.

Monterey, California. Naval Postgraduate School

---

<http://hdl.handle.net/10945/3971>

---

*Downloaded from NPS Archive: Calhoun*



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

<http://www.nps.edu/library>



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**A REVITALIZED INFORMATION ASSURANCE  
TRAINING APPROACH AND INFORMATION  
ASSURANCE BEST PRACTICE RULE SET**

by

James A. Pappas

September 2008

Thesis Advisor:  
Second Reader:

Terry E. Smith  
Ray Elliott

**Approved for public release; distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> September 2008	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE</b> A Revitalized Information Assurance Training Approach and Information Assurance Best Practice Rule Set			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> LT James A. Pappas, USN				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b>  <p>As the Information Age emerges to become the next great technological movement of modern civilization, the passion for information dominance will ultimately lead to the possession of information superiority, yet inferiority could prevail in the same breath if not carefully examined. Unlike wars of the past, the DoD faces a new dimension to modern warfare, against a novel adversary: the faceless foe. This faceless foe can come from abroad, domestically, and even within our own seemingly secure, yet vulnerable infrastructure. As modern society continues to move forward with the "latest high-tech gadget" or "cutting edge" technology, information still prevails. With increased wants and needs for information comes the associated risks and vulnerabilities of information management as people (and organizational procedure) can work against you and/or your information management and protection schemes.</p> <p>The objective of this thesis is to assess the People and Organizational (P-O) aspect of secure network environments with respect to the current standards and procedures that the DoD implements toward protecting network infrastructures. This thesis aims to revitalize IA training standards and implement best practice methods to address the people (as users) and organizational procedures (as operating environment) influences within the DoD structure on information security.</p>				
<b>14. SUBJECT TERMS</b> Type Keywords Here Information Assurance, Information Operations, Information Warfare, infrastructure, computer security, OPSEC, insider attack, internet, computer network operations, information, best practice, network, training, security			<b>15. NUMBER OF PAGES</b> 101	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**A REVITALIZED INFORMATION ASSURANCE TRAINING APPROACH AND  
INFORMATION ASSURANCE BEST PRACTICE RULE SET**

James A. Pappas  
Lieutenant, United States Navy  
B.S., United States Naval Academy, 2000

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS  
ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2008**

Author: James A. Pappas

Approved by: Terry E. Smith  
Thesis Advisor

Ray Elliott  
Second Reader

Dr. Dan Boger  
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

As the Information Age emerges to become the next great technological movement of modern civilization, the passion for information dominance will ultimately lead to the possession of information superiority, yet inferiority could prevail in the same breath if not carefully examined. Unlike wars of the past, however, the Department of Defense (DoD) faces a new dimension to modern warfare, against a novel adversary: the faceless foe. This faceless foe can come from abroad, domestically, and even within our own seemingly secure, yet vulnerable infrastructure. As modern society continues to move forward with the “latest high-tech gadget” or “cutting edge” technology, information still prevails. With increased wants and needs for information comes the associated risks and vulnerabilities of information management as people (and organizational procedure) can work against you and/or your information management and protection schemes.

With the rapid growth of the internet and the expansion of the Global Information Grid (GIG), the US military and DoD agencies have unfortunately become the prime targets of numerous attacks from threats, both within and beyond the confines of the United States. The internet growth has also led to internet dependencies that will most likely continue to grow as well. Global awareness and standard operating procedures need to be incorporated by all users within these boundaries to provide the DoD with the assurance that their information will not be compromised, or perhaps sold to our adversaries.

The objective of this thesis is to assess the People and Organizational (P-O) aspect of secure network environments with respect to the current standards and procedures that the DoD implements toward protecting network infrastructures. This thesis aims to revitalize Information Assurance training standards and implement best practice methods to address the people (as users) and organizational procedures (as operating environment) influences within the DoD structure on information security.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>OVERVIEW .....</b>	<b>1</b>
<b>B.</b>	<b>OBJECTIVE .....</b>	<b>2</b>
<b>C.</b>	<b>METHODOLOGY .....</b>	<b>3</b>
<b>D.</b>	<b>THESIS ORGANIZATION.....</b>	<b>4</b>
<b>II.</b>	<b>LITERATURE REVIEW .....</b>	<b>7</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>7</b>
<b>B.</b>	<b>INFORMATION OPERATIONS .....</b>	<b>7</b>
1.	Computer Network Operations (CNO) .....	9
2.	Operations Security (OPSEC) .....	10
3.	Information Assurance (IA).....	10
<b>C.</b>	<b>DOD PUBLICATIONS: PEOPLE-ORGANIZATIONAL (P-O) ASPECT.....</b>	<b>11</b>
1.	DoD Directive 8500.1E: Information Assurance (IA) .....	11
2.	DoD Directive 8500.2: Information Assurance Implementation. ....	13
3.	Joint Publication 3-13: Information Operations.....	13
4.	The National Strategy to Secure Cyberspace.....	13
5.	Joint Publication 3-54: Joint Doctrine for Operations Security...15	
<b>D.</b>	<b>STANDARDS USED TO GOVERN AND MANDATE DOD &amp; COMMERCIAL INFRASTRUCTURES.....</b>	<b>15</b>
1.	NIST 800-18: National Institute of Standards and Technology, Guide for Developing Security Plans for Federal Information Systems.....	15
2.	FIPS Pub-199: Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems.....	16
3.	Federal Information Security Management Act of 2002 (FISMA).....	17
4.	Director of Central Intelligence Directive, DCID 6/3: Protecting Sensitive Compartmented Information within Information Systems Manual.....	18
5.	DoD Directive 5200.40: Defense Information Technology Security Certification and Accreditation Process (DITSCAP).....	18
6.	Office of Management and Budget (OMB) Circular A-130 & Appendix III .....	19
<b>E.</b>	<b>CYBER-PLAYERS INVOLVED .....</b>	<b>20</b>
1.	Federal Bureau of Investigation (FBI).....	20
2.	Department of Homeland Security (DHS).....	21
3.	Department of Defense (DoD).....	21
<b>F.</b>	<b>LITERATURE REVIEW ANALYSIS .....</b>	<b>24</b>

III.	THE INNER PROBLEM OF INFORMATION MANAGEMENT .....	26
A.	THE WORLD WIDE WEB (INTERNET).....	27
1.	Introduction.....	27
2.	Internet Users by the Numbers.....	27
3.	The Growth of the Internet.....	30
B.	THE INSIDER ATTACK .....	32
C.	OFFICE OF MANAGEMENT AND BUDGET: FISMA REPORTS (FEDERAL INFORMATION SECURITY MANAGEMENT ACT).....	33
1.	Fiscal Year 2005 FISMA Results.....	35
2.	Fiscal Year 2007 FISMA Results.....	36
D.	RECAP.....	40
IV.	REVITALIZED INFORMATION ASSURANCE APPROACH.....	41
A.	INTRODUCTION.....	41
B.	IA AWARENESS TRAINING .....	42
1.	The Current Method.....	42
2.	A New Hope .....	44
a.	<i>Step 1: Incorporate Feedback and Question &amp; Answer Criteria.....</i>	44
b.	<i>Step 2: Increase IA Currency Requirements .....</i>	45
c.	<i>Step 3: Time Minimum .....</i>	46
d.	<i>Step 4: “90-Day” Specifics .....</i>	46
e.	<i>Step 5: The Consequences for Non-Compliance .....</i>	47
C.	BEST PRACTICE IA TECHNIQUES .....	48
1.	Best Practice Source 1: Common Risks Impeding the Adequate Protection of Government Information (via FISMA) ..	48
a.	<i>Risk 1 of 10: Security and Privacy Training is Inadequate and Poorly Aligned with the Different Roles and Responsibilities of Various Personnel .....</i>	49
b.	<i>Risk 5 of 10: Suspicious Activities and Incidents are Not Identified and Reported in a Timely Manner .....</i>	49
c.	<i>Risk 6 of 10: Audit Trails Documenting how Information is Processed are Not Appropriately Created or Reviewed .....</i>	50
d.	<i>Risk 7 of 10: Inadequate Physical Security Controls .....</i>	50
e.	<i>Risk 8 of 10: Information Security Controls are Not Adequate .....</i>	50
f.	<i>Risk 9 of 10: Inadequate Protection of Information Accessed or Processed Remotely .....</i>	51
2.	Best Practice Source 2: Common Sense Guide to Cyber Security for Small Businesses .....	51
3.	Best Practice Source 3: Build Security in: Training and Awareness .....	52
4.	Best Practice Source 4: Common Sense Guide to Prevention and Detection of Insider Threats .....	53
5.	Information Assurance Best Practice Rule Set .....	54
a.	<i>Physical Rule Set.....</i>	54

	<i>b.</i>	<i>Training Rule Set</i> .....	54
	<i>c.</i>	<i>Informational Rule Set</i> .....	55
	<i>d.</i>	<i>Procedural</i> .....	55
<b>D.</b>		<b>RECAP</b> .....	56
<b>V.</b>		<b>ANALYSIS, RECOMMENDATIONS AND EVALUATION METRICS</b> .....	57
<b>A.</b>		<b>INTRODUCTION</b> .....	57
<b>B.</b>		<b>KEY FEATURES</b> .....	58
	<b>1.</b>	<b>Publications</b> .....	58
	<b>2.</b>	<b>Information Assurance Training</b> .....	58
	<i>a.</i>	<i>Feature 1: Comprehension of IA Knowledge</i> .....	59
	<i>b.</i>	<i>Feature 2: Currency Requirements</i> .....	59
	<i>c.</i>	<i>Feature 3: Consequences for Violations</i> .....	59
	<b>3.</b>	<b>Information Assurance Best Practice Rule Set</b> .....	60
	<i>a.</i>	<i>Feature 1: Physical Rule Set</i> .....	60
	<i>b.</i>	<i>Feature 2: Training Rule Set</i> .....	60
	<i>c.</i>	<i>Feature 3: Informational Rule Set</i> .....	61
	<i>d.</i>	<i>Feature 4: Procedural Rule Set</i> .....	61
<b>C.</b>		<b>RECOMMENDATIONS</b> .....	61
	<b>1.</b>	<b>Authorize the Revitalized Approach</b> .....	61
	<b>2.</b>	<b>Implement IA Best Practice Rule Set</b> .....	62
<b>D.</b>		<b>SAFE-USER MODEL</b> .....	63
<b>E.</b>		<b>VALIDATION OF THE RECOMMENDATIONS</b> .....	64
	<b>1.</b>	<b>Validation Metrics</b> .....	65
	<b>2.</b>	<b>Proposed Acceptance Criteria</b> .....	67
<b>F.</b>		<b>POSSIBLE SHORTCOMINGS</b> .....	68
<b>G.</b>		<b>RECAP</b> .....	68
<b>VI.</b>		<b>CONCLUSION</b> .....	71
<b>A.</b>		<b>SUMMARY</b> .....	71
<b>B.</b>		<b>SUGGESTIONS FOR FUTURE RESEARCH</b> .....	72
	<b>1.</b>	<b>Certification and Accreditation</b> .....	72
	<b>2.</b>	<b>Develop Measures</b> .....	72
	<b>3.</b>	<b>Evaluate the Validation</b> .....	73
	<b>4.</b>	<b>OPSEC Model</b> .....	73
<b>APPENDIX</b>		<b>IA TRAINING SAMPLE QUESTIONS</b> .....	75
		<b>LIST OF REFERENCES</b> .....	78
		<b>INITIAL DISTRIBUTION LIST</b> .....	85

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	2007 CSI Survey Statistics .....	20
Figure 2.	Internet Users by Country (Volume) .....	27
Figure 3.	Internet Users by Country (Percentage).....	28
Figure 4.	Internet Users in the World Growth 1995-2010 .....	30
Figure 5.	Number of Major Agencies Reporting Weaknesses in Control Categories ....	38
Figure 6.	DoD IA Training Start-Up Page .....	42
Figure 7.	Sample IA Training Page .....	43
Figure 8.	Safe-User Model .....	64

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Information Operations (IO) Capabilities .....	9
Table 2.	Information Assurance (IA) Key Terminology .....	11
Table 3.	Potential Impact Definitions for Security Objectives .....	17
Table 4.	Internet Users Rankings by Number .....	29
Table 5.	Growth of Internet Users (1995-2008) .....	31
Table 6.	FISMA Scoring Categories.....	34
Table 7.	FY2001-FY2005 Federal Computer Security Grades (FISMA) .....	35
Table 8.	FY2007 Federal Computer Security Grades (FISMA) .....	36
Table 9.	Metrics for Validation.....	66

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

I would like to thank my wonderful wife, Kelly, who began her nursing career here in Monterey, for understanding me when times were stressful, supporting me and encouraging me throughout this process. Without her love and support, I would have struggled to finish the IW curriculum, or develop the concepts described in this thesis. I would like to thank my children, Anthony and Mary, for being there for me and being my inspiration to finish everything on time and complete. We had many good times and long lasting memories during our time on the Monterey Peninsula.

Finally, I would like to thank Lt. Col. Smith for his mentorship and guidance throughout the entire thesis process and willingness to assist me when especially during crunch time.

THIS PAGE INTENTIONALLY LEFT BLANK

# **I. INTRODUCTION**

## **A. OVERVIEW**

As the Information Age emerges to become the next great technological movement of modern civilization, the passion for information dominance will ultimately lead to the possession of information superiority, yet inferiority could prevail in the same breath if not carefully examined. During the Cold War era, the Department of Defense (DoD) was fully engaged in a massive nuclear arms race with a well known enemy, like that of the former Soviet Union, in order to preserve national security. Likewise, with the recent technological advances and the speedy growth of the Internet, we are now entering a new race for national security or in some cases, business enterprise security; both include the race for superior information management. Unlike wars of the past, the DoD faces a new dimension to modern warfare against a novel adversary: the faceless foe.

This faceless foe can come from abroad, domestically, and even within our own seemingly secure, yet vulnerable infrastructure. As modern society continues to move forward with the “latest high-tech gadget” or “cutting edge” technology, information still prevails. With increased wants and needs for information comes the associated risks and vulnerabilities of information management as people (and organizational procedure) can work against you and/or your information management and protection schemes.

Currently, the Department of Defense (DoD) is struggling with managing information flow. As the DoD information infrastructure grows on a daily basis, constant cyber-attacks, cyber-crimes and exploitations are being uncovered at an alarming rate.<sup>1</sup> So with that being said, many questions about DoD Information Assurance (IA) and Operations Security (OPSEC) effectiveness come to the surface. For example, are current computer network defense procedures and principles meeting the mark in safeguarding government installations from cyber crimes/attacks? Perhaps, the principal interest may be that computer network defense procedures and principles are in position,

---

<sup>1</sup> Internet Crime Complaint Center (IC<sup>3</sup>), *2007 Internet Crime Report*, National White Collar Crime Center: Federal Bureau of Investigation (FBI). Washington D.C. 2007.  
[http://www.nw3c.org/research/site\\_files.cfm?mode=p](http://www.nw3c.org/research/site_files.cfm?mode=p) (Last accessed 05 September 2008).

but rather the people (users) are the ones inducing the tribulations and vulnerabilities within the DoD information infrastructure.

With the rapid growth of the internet and the expansion of the Global Information Grid (GIG), the US military and DoD agencies have unfortunately become the prime targets of numerous attacks from threats, both within and beyond the confines of the United States. The internet growth has also led to internet dependencies that will most likely continue to grow. Global awareness and standard operating procedures need to be incorporated by all users within these boundaries to provide the DoD with the assurance that their information will not be compromised, or perhaps sold to our adversaries. The Commander in Chief's *National Strategy to Secure Cyberspace*<sup>2</sup> and the NETWARCOM mission (to create war-fighting and business options for the Fleet to fight and win in the information age)<sup>3</sup> address numerous protection areas that require critical analysis and revision or modifications to establish "best practice" rule sets to provide a more secure network environment. This thesis explores new approaches towards Information Assurance (IA) training and the necessary best practice methods to address the people (as users) and organizational procedures (as operating environment) influences within the DoD structure on information security.

## **B. OBJECTIVE**

The underlying factor garnering all the elements of information management is the influence of the people who create and/or use information. People influence the array of information we desire and intend to use, whether in the military or civilian market. People are the operators of the computers, machines or devices, influencing what is produced, collected, disseminated, interpreted, and ultimately acted upon to make decisions. People are also the foundations of potential strengths and weaknesses within a given network or information infrastructure. In the end, people are the ancestral roots of

---

<sup>2</sup> President of the United States, *The National Strategy to Secure Cyberspace*. United States: The White House, Washington D.C. 2003.

[http://www.dhs.gov/xlibrary/assets/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf) (Last accessed 05 September 2008)

<sup>3</sup> *Naval Network Warfare Command (NETWARCOM) Strategic Plan 2006-2010 (Version 2.1)*, NETWARCOM, Norfolk, VA. 1 November 2007. <http://www.netwarcom.navy.mil/> (Last accessed 16 July 2008).

information management (good or bad) and their influence inherently frames the nature and effectiveness of how an infrastructure or installation envisions information security.

The objective of this thesis is to assess the People and Organizational (P-O) aspect of secure network environments with respect to the current standards and procedures that the Department of Defense implements toward protecting network infrastructures. To be more specific, how will the DoD revive Information Assurance training standards and assure a “best practice” model that streamlines procedures while at the same time minimizing the potential for compromising integrity related to critical information flow? Finally, how can we be assured of a sustained safe level of network operations in support of critical mission requirements?

### **C. METHODOLOGY**

To assess the impact of the P-O influence on the DoD infrastructure, an in-depth literature review (procedures, doctrines, and standards), internet searches, etc. were conducted. The literature review included DoD Publications relating to the P-O influence on networks such as *DoD Directive 8500.1 & 8500.2: IA and Implementation*, *JP 3-13: Joint Doctrine for Information Operations*, *CSI/FBI Computer Crime and Security Survey*, *Department of Justice, JP 3-54: Joint Doctrine for Operations Security*, *The National Security Strategy to Secure Cyberspace*, additional DoD publications and various articles and non-DoD publications. Additionally, the literature review explored the current standards used to govern & mandate DoD and commercial personnel, installations and infrastructures to preserve the integrity of our information sources. Such documents included: *NIST 800-18: National Institute of Standards and Technology*, *FIPS-199: Information Processing Standards Publication*, *DCID 6/3: Director of Central Intelligence Directive*, *DoD Directive 5200.40: DITSCAP*, and other thesis, reports, or documentation relating to the P-O influence and the relationships between the P-O influence and information assurance policies and practices. Lastly, the analysis identifies the major players involved in the struggle for preserving information management.

Next, the analysis examined the information management dilemma, established a baseline addressing areas of concern and interest with respect to enhancing the People/User role in attaining a safe information infrastructure. Additionally, current practices and techniques utilized to uphold DoD and commercial information infrastructures were investigated.

Finally, using all described information sources, current DoD measures were critically analyzed to illustrate how the DoD and the various governmental agencies could potentially establish a safe-user infrastructure model to thwart exploits and attacks from ongoing cyber attacks/crimes. Best practices, DoD and commercial techniques were evaluated to develop a conceptual design for streamlining the people/user effects (including second and third order effects) to a network infrastructure. Following evaluation and assessment, the analysis will be used to develop performance metrics for testing and evaluation in order to validate the best information management practices that can be employed in DoD installations or infrastructures to deter corruption from within a network.

#### **D. THESIS ORGANIZATION**

This thesis consists of six chapters with respect to the People and Organizational criterion effect on network security and with focused emphasis on DoD Information Assurance (IA) and OPSEC. Chapter II examines the history, origins, terms & definitions, and all pertinent documents/publications currently in use with respect to the P-O aspect towards minimizing loss or damages to the DoD network or information infrastructure. Furthermore, Chapter II also discusses the role of the various federal agencies and DoD branches through IA and OPSEC. Chapter III focuses on the insider threat as a specific area of concern. In addition, Chapter III investigates and analyzes the Federal Information Security Management Act (FISMA) report(s) used to evaluate the various governmental departments. Chapter IV proposes a revitalized approach to the current IA awareness training and introduces an IA best practice rule set to be further implemented toward all installations to counter inside/outside cyber attacks. Chapter V investigates and makes recommendations based on the two IA approaches from Chapter IV with respect to the P-O aspect. Additionally, Chapter V looks to bring forth the

potential to alleviate risks and vulnerabilities by introducing a Safe-User model and metrics for evaluation and concepts for network protection success. Chapter VI provides conclusions and recommendations for future work. The final chapter also expands on those informational areas involving the Information Operations (IO) areas that consist of Computer Network Defense, Information Assurance and/or Operational Security.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. LITERATURE REVIEW**

### **A. INTRODUCTION**

The documents cited in this chapter represent only an elite selection of the various works studied and referenced throughout the remainder of this thesis. Each principle source is critiqued with a brief synopsis describing the guidance and purpose for information management features with respect to aspects that address the influence of the people and organizational procedures. Lastly, Chapter II focuses on defending the notion that current standards, policies and procedures are abundant, and often redundant, constantly re-emphasizing similar best practice principles, both in the federal and civilian sphere of influence.

The blueprint for Chapter II is to explore the function of Information Operations and the various security elements IO encompasses. Next, the various DoD Publications relating to the People-Organizational Influence are examined, followed by the standards used to govern and mandate DoD and Commercial Infrastructures. Lastly, a depiction of the cyber-players involved is included to show the enormity of this growing problem with cyber security with respect to the people or organizational influence.

### **B. INFORMATION OPERATIONS**

Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities. Joint Publication 3-13: *Information Operations*, is the governing doctrine that categorizes the role of Information Operations (IO) in today's environment to help combatant commanders prepare, plan, execute, and assess IO in support of joint operations.

JP-3-13 defines IO as:

The integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.<sup>4</sup>

The overall goal is to achieve information superiority for the United States and its coalition partners. As per U.S. Air Force Doctrine Document 2-5: *Information Operations*, information superiority is defined as:

The degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.<sup>5</sup>

The focus of this thesis expands on computer network operations (CNO) and operations security (OPSEC) concepts, two of the five core IO capabilities, with heavy emphasis on Information Assurance (IA), one of five supporting IO capabilities. One can view IO via these three capabilities as a wire mesh. Throughout the mesh, paths will cross and uncross creating a linked-network, but in the end a common goal is desired. The goal in this case is, through robust information infrastructure, policy and procedure to attain superiority of information and to assure the flow of information as a key enabler to command and control. The work here has a focus that expands beyond external threats to considerations of “protecting our own” infrastructures from being exploited and corrupted via various threats, both internal and external.

---

<sup>4</sup> Joint Publication (JP) 3-13: *Information Operations (IO)*, United States: Chairman, Joint Chiefs of Staff, Washington, D.C. February 13, 2006, I-1.

<sup>5</sup> Air Force Doctrine Document 2-5: *Information Operations*, United States: Department of Defense, Washington D.C. 11 January 2005, 1.

Many of the capabilities of Information Operations interact with one another as described above. The table below illustrates the IO capabilities divided between the Core, Supporting and Related capabilities emphasizing (highlighted yellow) the three facets of IO (CNO, OPSEC, and IA) for this thesis.<sup>6</sup>

<b>Information Operations (IO) Capabilities</b>		
<b>Core</b>	<b>Supporting</b>	<b>Related</b>
Electronic Warfare (EW)	Information Assurance (IA)	Civil Military Operations (CMO)
Computer Network Operations (CNO)	Physical Attack	Public Affairs (PA)
Psychological Operations (PSYOP)	Physical Security	Defense Support to Public Diplomacy (DSPD)
Military Deception (MILDEC)	Counter Intelligence (CI)	
Operations Security (OPSEC)	Combat Camera (COMCAM)	

Table 1. Information Operations (IO) Capabilities

## 1. Computer Network Operations (CNO)

CNO is one of the latest capabilities developed in support of military operations. CNO stems from the increasing use of networked computers and supporting IT (Information Technology) infrastructure systems by military and civilian organizations.<sup>7</sup> CNO is divided into three main sub-categories: CNA (Computer Network Attack), CNE (Computer Network Exploitation), and lastly CND (Computer Network Defense). The three CNO categories are described below:<sup>8</sup>

- CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

---

<sup>6</sup> Joint Publication (JP) 3-13: *Information Operations*, I-7.

<sup>7</sup> Ibid., II-4.

<sup>8</sup> Ibid.

- CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
- CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. CND actions not only protect DoD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations.

## **2. Operations Security (OPSEC)**

OPSEC is the process of identifying critical information and subsequently analyzing friendly actions and other activities to: identify what friendly information is necessary for the adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remain secure.<sup>9</sup>

## **3. Information Assurance (IA)**

IA is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.<sup>10</sup> As per Joint Pub 3-13, IA is necessary to gain and maintain information superiority. Furthermore, IA is assured in DoD systems by imposing requirements for a defense-in-depth approach that integrates the capabilities of people, operations, and technology to establish multilayer and multidimensional protection to ensure survivability and mission accomplishment. IA

---

<sup>9</sup> Joint Publication (JP) 3-54: *Operations Security (OPSEC)*, United States: Chairman, Joint Chiefs of Staff, Washington D.C. 2006, I-1.

<sup>10</sup> DoD Directive 8500.01E: *Information Assurance (IA)*. United States: Department of Defense, Washington D.C. 23 April 2007, 17.

must assume that access can be gained to information and information systems from inside and outside DoD-controlled networks.<sup>11</sup>

The Committee of National Security Systems (CNSS) defines the key terms commonly used for Information Assurance. Confidentiality, Integrity, and Availability (C.I.A.) are the three most commonly used IA attributes. These key terms and others are described below.<sup>12</sup>

Information Assurance (IA) Key Terminology	
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Integrity	Quality of an Information System reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware & software; and the consistency of the data structures and occurrence of the stored data.
Availability	Timely, reliable access to data and information services for authorized users.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Non-Repudiation	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Table 2. Information Assurance (IA) Key Terminology

## C. DOD PUBLICATIONS: PEOPLE-ORGANIZATIONAL (P-O) ASPECT

### 1. DoD Directive 8500.1E: Information Assurance (IA)

DoD Directive 8500.1E establishes the IA policy and assigns responsibilities to achieve DoD Information Assurance through a defense-in-depth approach that integrates

---

<sup>11</sup> Joint Publication (JP) 3-13: *Information Operations*, II-6.

<sup>12</sup> CNSSI (Committee on National Security Systems Instruction) 4009: *National Information Assurance Glossary*, National Security Agency, Ft. Meade, MD, 2003, 4-34.

the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. Below are a few key policies found in DoD 8500.1E:<sup>13</sup>

- All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness.
- Interoperability and integration of IA solutions within or supporting the DoD shall be achieved through adherence to an architecture that will enable the evolution to network centric warfare by remaining consistent with the C4I, ISR architecture framework, and a defense in-depth approach.
- The DoD shall organize, plan, assess, train for, and conduct the defense of DoD computer networks as integrated computer network defense (CND) operations that are coordinated across multiple disciplines.
- Information assurance readiness shall be monitored, reported, and evaluated as a distinguishable element of mission readiness throughout all the DoD Components, and validated by the DoD CIO (Chief Information Officer).

---

<sup>13</sup> DoD Directive 8500.01E: *Information Assurance (IA)*, 3-4.

## **2. DoD Directive 8500.2: Information Assurance Implementation**

DoD Directive 8500.2 describes the roles and responsibilities for a network information and knowledge manager, IA Officer, down to the everyday individual user. Mostly stressing the roles and responsibilities of the network manager, room still exists for improvement in the roles, responsibilities and consequences for everyday user. Additionally, 8500.2 lists and describes all IA Controls (divided between the C.I.A. categories) needed to be incorporated throughout an installation's network security plan to enhance network security.<sup>14</sup> A more precise description of a security plan is presented in section D.1.

## **3. Joint Publication 3-13: Information Operations**

JP 3-13 is described above in Section A illustrating the various elements comprised of Information Operations. From the introduction of IO, each element can be further broken down by Core, Supporting and Related capability for a more enhanced understanding. CNO, OPSEC, and IA are the main focus in this thesis.

## **4. The National Strategy to Secure Cyberspace**

The *National Strategy to Secure Cyberspace* was released in February 2003 by the President of United States to guide the DoD and the various agencies, in unison with the public and private sectors, to improve cyberspace related concerns. The *National Strategy to Secure Cyberspace* identified several major priorities needed for action:<sup>15</sup>

- Priority I: A National Cyberspace Security Response System.
- Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program.
- Priority III: A National Cyberspace Security Awareness and Training Program.

---

<sup>14</sup> DoD Directive 8500.2: *Information Assurance (IA) Implementation*. United States: Department of Defense, Washington D.C. 2003, 25.

<sup>15</sup> President of the United States, *The National Strategy to Secure Cyberspace*, 3-4.

- Priority IV: Securing Governments' Cyberspace.
- Priority V: National Security and International Cyberspace Security Cooperation.

Expanding from the five priorities listed above, *The National Strategy to Secure Cyberspace* specified explicit programs and initiatives requiring action in response to cyberspace security. Below lists the explicit actions with the associated priority:<sup>16</sup>

- Establish a public and private architecture for responding to national-level cyber incidents. (Priority I)
- Exercise cybersecurity continuity plans for federal systems. (Priority I)
- Enhance law enforcement's capabilities for preventing and prosecuting cyberspace attacks. (Priority II)
- Promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace. (Priority III)
- Foster adequate training and education programs to support the Nation's cybersecurity needs. (Priority III)
- Increase the efficiency of existing federal cybersecurity training programs. (Priority III)
- Continuously assess threats and vulnerabilities to federal cyber systems. (Priority IV)
- Work with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures. (Priority V)

---

<sup>16</sup> President of the United States, *The National Strategy to Secure Cyberspace*, 19-52.

## **5. Joint Publication 3-54: Joint Doctrine for Operations Security**

Similar to the description given in section B.2., Operations Security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations to:<sup>17</sup>

- Identify those actions that can be observed by adversary intelligence systems.
- Determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC's most important characteristic is that it is a process and not a collection of specific rules and instructions that can be applied to every operation.<sup>18</sup> Therefore, OPSEC and security programs must be closely synchronized to ensure that all features of sensitive operations are protected.

## **D. STANDARDS USED TO GOVERN AND MANDATE DOD AND COMMERCIAL INFRASTRUCTURES**

### **1. NIST 800-18: National Institute of Standards and Technology, Guide for Developing Security Plans for Federal Information Systems**

The objective of NIST 800-18 is to lay the framework for system security planning for any installation in order to improve the protection of information system resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behaviors of all individuals who access the system. The system security

---

<sup>17</sup> Joint Pub 3-54: Joint Doctrine for Operations Security (OPSEC), I-1.

<sup>18</sup> Ibid.

plan should be viewed as the documentation of the structured process of planning adequate, cost-effective security protection for a system.<sup>19</sup> A system security plans includes:

- Security requirements.
- Current defensive postures.
- Plans for future changes.
- Responsibilities and expected behaviors of the users, administrators, and managers.

## **2. FIPS Pub-199: Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems**

FIPS-199 is the mandatory standard to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to impact (refer to Table 3).<sup>20</sup> Security categorization standards for information and information systems provide a common framework and understanding for expressing security that the federal government promotes:<sup>21</sup>

- Effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities.
- Consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

---

<sup>19</sup> Pauline Bowen, Joan Hash and Marianne Swanson. NIST (National Institute of Standards and Technology) Special Publication 800-18, Information Security: *Guide for Developing Security Plans for Federal Information Systems*, United States: Department of Commerce, Gaithersburg, MD, 2006, vii.

<sup>20</sup> FIPS Pub-199, Federal Information Processing Standards Publication: *Standards for Security Categorization of Federal Information and Information Systems*, United States: Department of Commerce, Gaithersburg, MD, 2004, 6.

<sup>21</sup> Pauline Bowen, Joan Hash and Marianne Swanson, 2.

Below, Table 3 reviews the potential impact definitions for the three (C.I.A.) security objectives:<sup>22</sup>

Potential Impact for Security Objectives			
Security Objective	Low	Moderate	High
<u>Confidentiality</u> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<u>Integrity</u> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<u>Availability</u> Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

Table 3. Potential Impact Definitions for Security Objectives

### 3. Federal Information Security Management Act of 2002 (FISMA)

The Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 emphasizing Information Security.<sup>23</sup> The act was meant to bolster computer and network security within the federal government and affiliated parties by mandating yearly audits.

<sup>22</sup> From: FIPS Pub-199, 2.

<sup>23</sup> United States Congress (107<sup>th</sup> Congress), H.R. 2458 Title III of the E-Government Act of 2002: *Information Security*, 44 U.S.C. § 3541, 2002. <http://uscode.house.gov/download/pls/44C35.txt> (Last accessed 20 August 2008).

FISMA has brought attention within the federal government to cybersecurity which had previously been much neglected. In February 2005, many government agencies received extremely poor marks on the official FISMA report card, with an average of 67.3% for 2004, an improvement of only 2.3 percentage points over 2003. Unfortunately, grades have not shown any substantial improvement showing signs of potential weaknesses. Chapter III will analyze the results of OMB's annual FISMA reports from 2005 and 2007.

**4. Director of Central Intelligence Directive, DCID 6/3: Protecting Sensitive Compartmented Information within Information Systems Manual**

United States intelligence information uses the same three FISMA attributes that require protection: Confidentiality, Integrity, and Availability. The degree of emphasis on each varies with the type of information processed and the mission of the organization responsible for the data. DCID 6/3 recognizes the contributions to security made by operating environments, and allows the technical safeguards of systems to be modified accordingly.<sup>24</sup>

**5. DoD Directive 5200.40: Defense Information Technology Security Certification and Accreditation Process (DITSCAP)**

The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) is the process defined by the United States Department of Defense (DoD) for managing risk. DITSCAP establishes a standard DoD-wide process with a set of activities, general tasks and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle. DITSCAP applies to the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997.<sup>25</sup>

---

<sup>24</sup> DCID 6/3, Director of Central Intelligence Directive 6/3: Protecting Sensitive Compartmented Information (SCI) within Information Systems Manual. 2000.

<sup>25</sup> DoD Instruction (DoDI) 5200.40: *Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*. United States: Department of Defense, Washington, DC: 1997.

## **6. Office of Management and Budget (OMB) Circular A-130 & Appendix III**

OMB Circular A-130, Management of Federal Information Resources, is one of many circulars produced by the United States Federal Government to establish policy for executive branch departments and agencies.<sup>26</sup> OMB Circular A-130 makes it mandatory for agencies and departments to implement the requirements of the Computer Security Act of 1987 and the Federal Information Security Management Act of 2002.<sup>27</sup> To date, FISMA has since superseded the requirements of the Computer Security Act of 1987.

Specific guidelines for OMB Circular A-130 require:

- All federal information systems to have security plans.
- Systems to have formal emergency response capabilities.
- A single individual to have responsibility for operational security.
- Security awareness training made available to all government users, administrators of the system.
- Regular review/improvement upon contingency plans to be done.

OMB Circular A-130 Appendix III establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-130.<sup>28</sup>

---

<sup>26</sup> OMB Circular A-130, *Management of Federal Information Resources*, United States: Office of Management and Budget, Washington D.C. 2000.  
<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html> (Last accessed 09 August 2008).

<sup>27</sup> The Computer Security Act of 1987 was passed by Congress to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. [http://en.wikipedia.org/wiki/Computer\\_Security\\_Act\\_of\\_1987](http://en.wikipedia.org/wiki/Computer_Security_Act_of_1987) (Last accessed 15 August 2008).

<sup>28</sup> OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*, United States: Office of Management and Budget, Washington, D.C. 2000.

## E. CYBER-PLAYERS INVOLVED

### 1. Federal Bureau of Investigation (FBI)

The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime.<sup>29</sup> The FBI has established a Cyber Operations workforce including Cyber Action Teams, Computer Crimes Task Forces, and Internet Crime Complaint Centers. Additionally, the FBI/CSI Computer Crime and Security Surveys were derived from this agency providing information and valuable statistics toward cyber crime.<sup>30</sup> Below is a set of results from the 2007 survey, illustrating the type of attacks an installation may most likely face.



Figure 1. 2007 CSI Survey Statistics <sup>31</sup>

<sup>29</sup> Role of FBI is defined via the FBI website. <http://www.fbi.gov/cyberinvest/cyberhome.htm> (Last accessed 15 August 2008).

<sup>30</sup> CSI is defined as the Computer Security Institute.

<sup>31</sup> From: Computer Security Institute (CSI) and the Federal Bureau of Investigation, *CSI/FBI Computer Crime and Security Survey*, United States: Department of Justice, Washington D.C. 2005. <http://www.fbi.gov/page2/july05/cyber072505.htm> (Last accessed 15 August 2008).

## **2. Department of Homeland Security (DHS)**

The Department of Homeland Security National Cyber Security Division (NCSD) works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets. The division is home to US-CERT (US Computer Emergency Readiness Team) operations and the National Cyber Alert System.<sup>32</sup> The DHS Science and Technology Directorate also help government and private end-users transition to new cyber-security capabilities. To protect the cyber infrastructure, NCSD has identified two main objectives. First they are to build and maintain an effective national cyber response system. Secondly, NCSD is to implement a cyber-risk Management program for protection of critical infrastructures.<sup>33</sup>

From the *National Strategy to Secure Cyberspace*, the DHS is responsible for developing the national cyberspace security response system, which includes providing crisis management support in response to threats to, or attacks on critical information systems. Additionally, DHS coordinates with other agencies of the federal government to provide specific warning information, and advice about appropriate protective measures and countermeasures, to state and local government agencies and authorities, the private sector, other entities, and the public.<sup>34</sup>

## **3. Department of Defense (DoD)**

The Department of Defense Cyber Crime Center (DC3) sets standards for digital evidence processing, analysis, and diagnostics for any DoD investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. DC3 remains on the leading edge of computer technologies and techniques

---

<sup>32</sup> Role of Department of Homeland Security (DHS) National Cyber Security DivisionDHS as defined from DHS website. [http://www.dhs.gov/xabout/structure/editorial\\_0839.shtm](http://www.dhs.gov/xabout/structure/editorial_0839.shtm) (Last accessed 22 August 2008).

<sup>33</sup> Role of Department of Homeland Security (DHS) National Cyber Security DivisionDHS as defined from DHS website. [http://www.dhs.gov/xabout/structure/editorial\\_0839.shtm](http://www.dhs.gov/xabout/structure/editorial_0839.shtm) (Last accessed 22 August 2008).

<sup>34</sup> President of the United States, *The National Strategy to Secure Cyberspace*, 20.

through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.<sup>35</sup>

The Defense Cyber Crime Institute (DCCI) provides legally & scientifically accepted standards, techniques, methodologies, research, tools, and technologies on computer forensics and related technologies to meet the current and future needs of the DoD counterintelligence, intelligence, information assurance, information operations, and law enforcement communities.<sup>36</sup>

The DoD military services also play a pivotal role in the cyberspace domain. The U.S. Air Force may soon stand up a new Air Force Cyber Command (starting on 1 October 2008) with the mission to secure the nation by employing world-class cyberspace capabilities to control cyberspace, create integrated global effects and deliver sovereign option.<sup>37</sup> The U.S. Army provides high quality virtual Information Assurance and Computer Network Defense training and certification for DoD personnel at Fort Gordon, Georgia.<sup>38</sup> Like the Army, the United States Marine Corps established an IA Division (based in Quantico, VA) to oversee and perform continuous assessment of USMC IA operations and resource expenditures to evaluate the extent to which policy objectives are being achieved.<sup>39</sup> Finally, the U.S. Navy developed an Information Assurance manual to analyze IA principles and controls that apply to the people, processes, and technology. The U.S. Navy IA program is set out to:

---

<sup>35</sup>The Mission of the Department of Defense Cyber Crime Center (DC3) <http://www.dc3.mil> (Last accessed 22 August 2008).

<sup>36</sup>*Ibid.*

<sup>37</sup> Air Force Cyberspace Command. <http://www.afcyber.af.mil> (Last accessed 05 September 2008)

<sup>38</sup> US Army Information Assurance Training Center. <https://ia.gordon.army.mil> (Last accessed 02 September 2008).

<sup>39</sup> USMC IA Headquarters. <http://www.quantico.usmc.mil/activities/?Section=IA> (Last accessed 02 September 2008).

Deliver secure, interoperable, and integrated information management and information technology to the Marine and Sailor to support the full spectrum of war-fighting and war-fighting support missions.<sup>40</sup>

---

<sup>40</sup> Secretary of the Navy, *SECNAV M-5239.1: Information Assurance Manual*, Department of the Navy, United States, November 2005, 3. [www.fas.org/irp/doddir/navy/secnavinst/m5239\\_1.pdf](http://www.fas.org/irp/doddir/navy/secnavinst/m5239_1.pdf) (Last accessed 02 September 2008).

## **F. LITERATURE REVIEW ANALYSIS**

The literature review of this thesis included approximately 30 documents and publications relating to information security, both from the governmental and civilian sectors. In general, the vast majority of the documents clearly depicted a ‘top-down’ approach, while very nominal amounts represented any ‘bottom-up’ perspectives and viewpoints towards information security. Most take the stance from a strategic point of view, when operational and tactical documents get pushed to the side. Redundancy was evident throughout the review, but the topic of day-to-day operations, is not addressed. In essence, the bulk of documents and publications are intended for the information/knowledge managers and the hierarchical information leadership, while minimal guidance is directed towards the user and his/her roles and responsibilities to maintain information stability. Virtually no guidance or framework is given to the countless operators/users, and that which is provided is often duplicated.

By evaluating all these works, even those not stated in Chapter II, there is an immense need for a ‘people-oriented users’ policy for managers to maintain when dealing with people influence and the organization procedural downfalls. Bottom level installations deal with occurrences of insider and outsider attacks daily. No standard is readily available for reference and neither is a standard metric system for measuring compliance. The shortcomings of this described environment, appears to provide fertile ground for ‘problems waiting to happen’.

Of the many documents reviewed, two documents stand out as ‘must reads’ for information and knowledge managers: OMB Circular A-130 and DoD 8500.1/2 (two documents working in unison). Both of these documents discuss the behaviors and responsibilities of the user, but users are not enforced to read such documents and no tracking and feedback method with respect to those that have completed the reading is currently in effect. Chapter III investigates the growth of the internet and the topic of internet dependency as a critical means of communication. Additionally, Chapter III focuses on the insider threat as the specific area of concern and analyzes the annual Federal Information Security Management Act (FISMA) reports.

The concluding chapters of this thesis will argue the case that a policy needs to be integrated with the existing network standards, focusing on the people influence by revitalizing the current Information Assurance training and implementing an IA best practice rule set. Additionally, metrics for validation will be introduced to evaluate the training and best practice methods with hopes to enhance user behaviors, awareness and responsibilities. Again, the people are the basic units of information, the people are the operators and the people control all the key mechanisms of a network, either directly or indirectly. Because of that heavy influence, the actions of the people need to be addressed and acted upon to improve IA awareness throughout the DoD.

THIS PAGE INTENTIONALLY LEFT BLANK

### III. THE INNER PROBLEM OF INFORMATION MANAGEMENT

#### A. THE WORLD WIDE WEB (INTERNET)

##### 1. Introduction

As the need for information continues to rise, so does the need for speed, accuracy, and content with respect to any information contained. With the World Wide Web connectivity growing by the second, nodes of strengths & weaknesses related to the information demand open at the same rate. The number of internet users has grown quickly over the years, allowing for more possibilities of cyber crimes/attacks. Although most users might not ever consider intentionally compromising a network's information or infrastructure (through hacking), some do, and therefore the potential is real.

##### 2. Internet Users by the Numbers

With the growth of the internet, mass numbers of online users are created everyday. Figure 2 depicts the number of internet users by country, illustrating the high volume and the specific concentrations of internet users throughout the world for 2007.

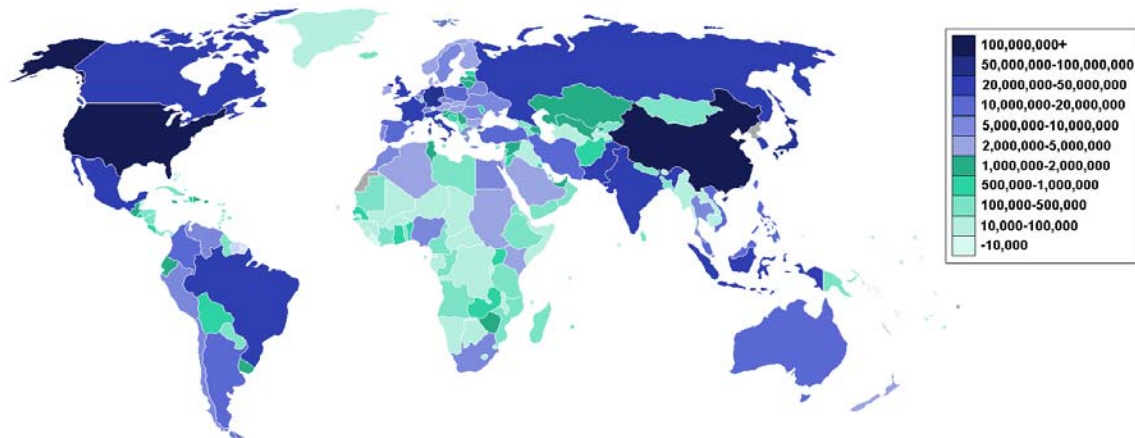


Figure 2. Internet Users by Country (Volume)<sup>41</sup>

<sup>41</sup> From: Internet Growth graphic found on Wikipedia search on Internet Growth by Country. [http://en.wikipedia.org/wiki/List\\_of\\_countries\\_by\\_number\\_of\\_Internet\\_users](http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users) (Last accessed 09 August 2008).

Additionally, some countries have shown a resounding dependency on internet use as the primary means of communication, both domestically and internationally. Of note (see Figure 2, 3), the United States, Canada, Australia, Japan and Europe (particularly the north Scandinavian Nations) validate this high concentration of users as a whole. The number of potential users also correlates to the number of potential attackers a nation may possess and/or encounter. This data does not conclude that hackers from one nation do not infiltrate infrastructures outside country lines; the user numbers simply illustrate the origin of potential damage. In fact, although the origin countries are noted, global connectivity is involved.

Figure 3 illustrates the number of internet users by country (via percentage of population) for the year 2007. These markets of heavy internet dependence reveal the strong relationships of the potential for internet user harm.

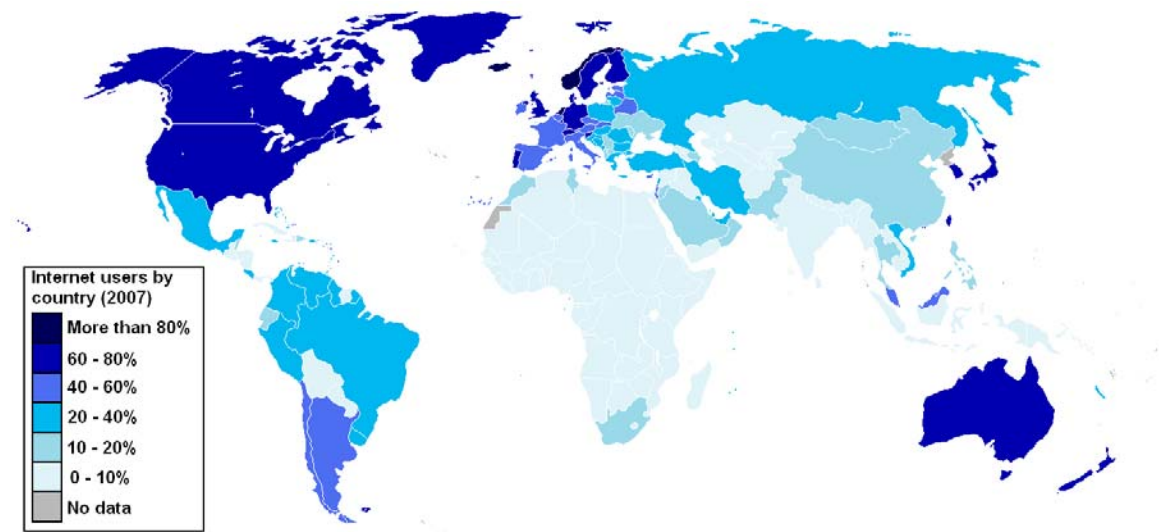


Figure 3. Internet Users by Country (Percentage)<sup>42</sup>

---

<sup>42</sup> From: Internet Growth graphic found on Wikipedia search on Internet Growth by Country. [http://en.wikipedia.org/wiki/List\\_of\\_countries\\_by\\_number\\_of\\_Internet\\_users](http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users) (Last accessed 09 August 2008).

Table 4 below lists the top ten countries for internet users ranked by the total number of internet users. The figure also complements Figure 3 and provides the respective country's percentage of the population depending on the internet as a line of communication.













Rank [1]	Country [2]	Internet users [3]	% of pop. [4]	Date [5]
—	 World	1,173,109,925	17.8%	2007
—	 European Union	273,234,619	55.7%	2007
1	 China	227,000,000	16.7%	2008
2	 United States	217,575,287	71.7%	2007
3	 Japan	86,300,000	67.1%	2007
4	 India	60,000,000	6.0%	2005
5	 Germany	52,533,914	63.8%	2008
6	 Brazil	50,000,000	26.1%	2008
7	 United Kingdom	37,600,000	62.3%	2007
8	 South Korea	34,910,000	71.2%	2007
9	 France	32,925,953	53.7%	2007
10	 Italy	31,481,928	52.9%	2007

Table 4. Internet Users Rankings by Number <sup>43</sup>

From this data set, the nations with the highest numbers and percentage of users come as no surprise. These nations are typically found leading the charge towards innovative and cutting edge technologies and pioneering industrial trends for the future.

<sup>43</sup> From: Internet Growth graphic found on Wikipedia search on Internet Growth by Country.  
[http://en.wikipedia.org/wiki/List\\_of\\_countries\\_by\\_number\\_of\\_Internet\\_users](http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users) (Last accessed 09 Aug 2008).

### 3. The Growth of the Internet

The growth of the Internet has drastically increased over the past 13 years. This was hard to imagine in 1995 when only 0.4% of the world's population had the capability to get globally connected. Figure 4 below illustrates the rapid growth of the internet, providing graphical and statistical data dating back to 1995 and projecting forward to 2010:

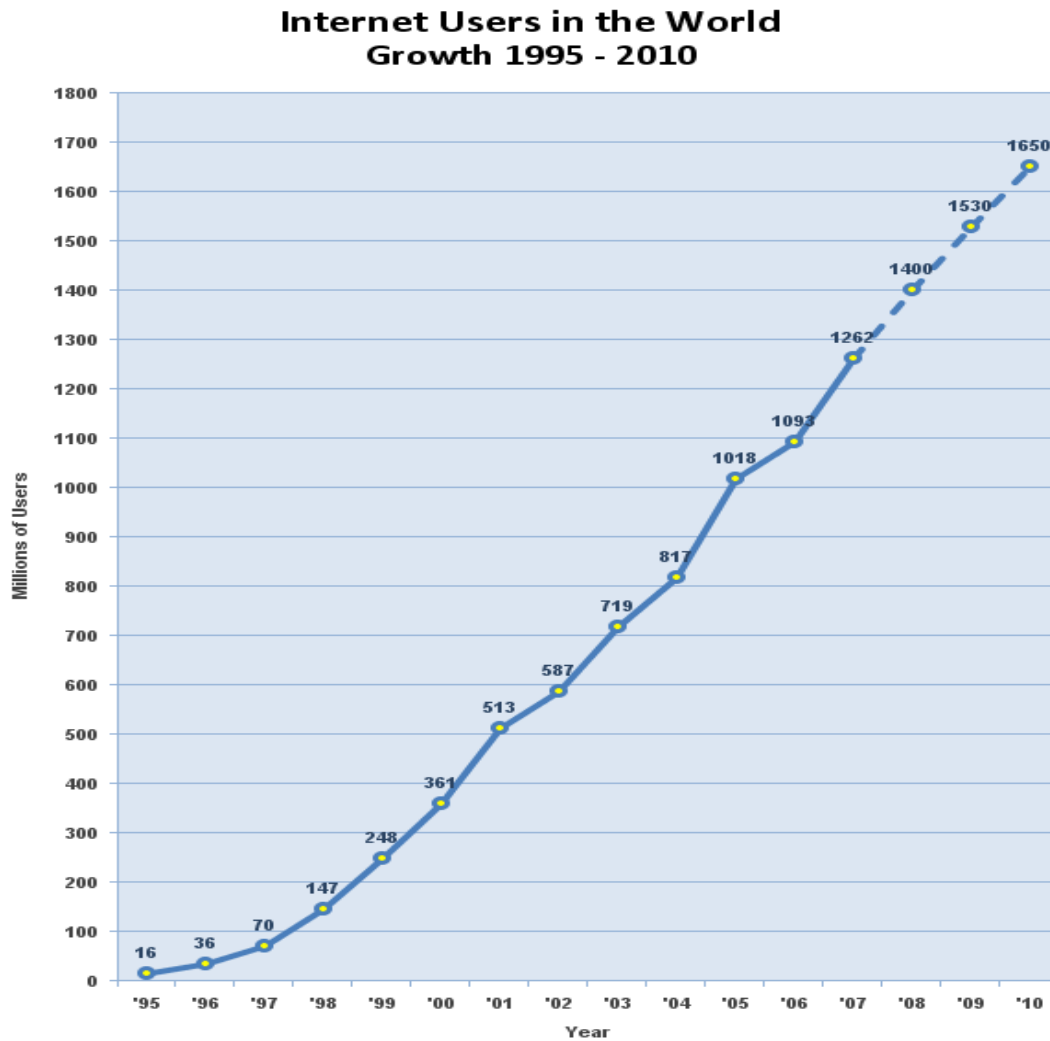


Figure 4. Internet Users in the World Growth 1995-2010 <sup>44</sup>

<sup>44</sup> From: Internet Users in the World Growth 1995-2010 figure found on <http://www.allaboutmarketresearch.com/internet.htm> (Last accessed 29 August 2008).

In conjunction with Figure 4 from above, Table 5 provides the approximate number of users, with the percentage of the world population from December 1995 to May 2008 and the percent growth since December 1995:

<b>Growth of Internet Users (1995-2008)</b>			
<b>Date</b>	<b>Number of Users</b>	<b>% World Population</b>	<b>% of Growth Since 1995</b>
December, 1995	16 million	0.40%	-
December, 1996	36 million	0.90%	225.00%
December, 1997	70 million	1.70%	437.50%
December, 1998	147 million	3.60%	918.70%
December, 1999	248 million	4.10%	1550.00%
December, 2000	361 million	5.80%	2256.20%
December, 2001	513 million	8.60%	3206.20%
December, 2002	587 million	9.40%	3668.70%
December, 2003	719 million	11.10%	4493.70%
December, 2004	817 million	12.70%	5106.20%
December, 2005	1,018 million	15.70%	6362.50%
December, 2006	1,093 million	16.70%	6831.20%
December, 2007	1,319 million	20.00%	8243.70%
May, 2008	1,412 million	21.20%	8825.00%

Table 5. Growth of Internet Users (1995-2008) <sup>45</sup>

The data above visibly illustrates an exponential-like growth of the internet over a rather short period in time. From 1995 to 1996, the number of internet users more than doubled from 16 million to 36 million with less than 1% of the world globally connected. From 1995 to 2000, the five year period indicated a growth of 2256.2% with 5.8% of the world's population having global connectivity. Finally, from 1995 to May 2008, the growth swelled 8825% with 21.2% of the world's population having global connectivity.

From this data, it's pretty easy to see that people have adopted the internet as a primary means of communication. Like the people, information infrastructures utilize the internet as a primary means of communication to collect, distribute and disseminate critical information to other host installations. As examples, people commonly pay their

---

<sup>45</sup> After: Internet Users in the World Growth 1995-2008 data found on <http://www.allaboutmarketresearch.com/internet.htm> (Last accessed 29 August 2008).

monthly bills via the internet, purchase items, do business with financial institutions and manage their retirement portfolios via the internet as well. From the perspective of the Department of Defense, critical mission related information is passed via the internet to coordinate among the many moving parts of most military operations. Protecting information is paramount for information security success.

## **B. THE INSIDER ATTACK**

In a recent study by the Secret Service, insider attacks on computers and networks are not rare occurrences. Most attacks are planned in advance. Insider attacks are the most detrimental within an information infrastructure. The statistics provided depict the scope of insider attacks from the commercial (non-DoD) sphere of influence.

Below are the statistics from the Secret Service study:<sup>46</sup>

- 80% of insiders who launched attacks on their companies had exhibited negative behaviors before the incident.
- 92% had experienced a negative work-related event, such as a demotion, transfer, warning or termination.
- At the time of the incident, 59% were former employees or contractors, while 41% were still on the company clock.
- Of the former employees, 48% had been fired, 38% had resigned and 7% had been laid off.
- 86% were employed in a technical position. Of them, 38% were system administrators.
- 21% were programmers, 14% were engineers and 14% were IT specialists
- 57% of insiders were perceived by others to be disgruntled.
- The majority of insiders compromised computer accounts, created unauthorized, backdoor accounts or used shared accounts in their attacks.

---

<sup>46</sup> Sharon Gaudin, "Study Highlights Insider Threats," *Information Week*, 25 August 2006. <http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=192300421> (Last accessed 05 September 2008).

The Insider threat can be the most detrimental to a company or governmental agency. The 2007 Computer Crime Survey indicated that 59% of the attacks on a network were classified as insider abuse.<sup>47</sup> Insiders do not need a great deal of knowledge about computer intrusion because their knowledge of the system often allows them to gain unrestricted access to cause damage to the system or steal system data.<sup>48</sup> Understanding that insiders and social engineering do exist is more than enough to label them a major concern.<sup>49</sup>

### **C. OFFICE OF MANAGEMENT AND BUDGET: FISMA REPORTS (FEDERAL INFORMATION SECURITY MANAGEMENT ACT)**

Each fiscal year, the Office of Management of Budget (OMB) conducts a yearly report evaluating the various departments of the US government on matters of computer security. The goals of the yearly FISMA reports are to evaluate the development of network security frameworks in order to protect the government's information, operations, and assets. The results of the annual FISMA report inform Congress (and the public) of the Federal government's security performance for a given fiscal year, while fulfilling the yearly OMB requirement.<sup>50</sup> Included in the reports are the strengths and weakness and plan of actions to improve performance.

---

<sup>47</sup> Internet Crime Complaint Center (IC<sup>3</sup>), *2007 Internet Crime Report*, 13.

<sup>48</sup> Gregory Wilshusen, *GAO-08-496T: Information Security Issues (FISMA Analysis)*, United States: US Government Accountability Office, Washington D.C. February 2008, 6.

<http://www.gao.gov/new.items/d08496t.pdf> (Last accessed 31 August 2008).

<sup>49</sup> Social engineering is the act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.

<sup>50</sup> Office of Management and Budget (OMB): *Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, United States: OMB, Washington D.C. 2007. <http://www.whitehouse.gov/omb/> (Last accessed 25 August 2008).

The six categories FISMA grades are as follows:

<b>FISMA Scoring Categories</b>	<b>Point Value</b>
Annual Testing	20
Plan of Action and Milestones (POA & M)	15
Certification and Accreditation	20
Configuration Management	20
Incident Detection and Response	15
Training	10
<b>Total</b>	<b>100</b>

Table 6. FISMA Scoring Categories

The FISMA letter grade distribution uses the following scale:

90 to 93 = A-	94 to 96 = A	97 to 100 = A+
80 to 83 = B-	84 to 86 = B	87 to 89 = B+
70 to 73 = C-	74 to 76 = C	77 to 79 = C+
60 to 63 = D-	64 to 66 = D	67 to 69 = D+
59 and lower = F		

Additionally, FISMA requires that agencies implement information security programs that, among other things, include:<sup>51</sup>

- Periodic assessments of the risk.
- Risk-based policies and procedures.
- Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate.
- Security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually.
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies.

---

<sup>51</sup> Gregory Wilshusen, 8.

- Procedures for detecting, reporting, and responding to security incidents.
- Plans and procedures to ensure continuity of operations.

Since the conception of the FISMA reporting standard, the Department of Defense has not shown any positive signs of improvement towards network security in any recent reports. The next section analyzes the FISMA reports.

## 1. Fiscal Year 2005 FISMA Results

The FY2005 FISMA computer security results were used as a reference point in this analysis to establish a baseline for network security compliance. The results from FY2005 and FY2007 were compared to analyze any positive or negative trends in the various departments in the FISMA report. DoD results were explicitly examined.

The FISMA report card for FY2005 to FY2001 (Table 7) presents the grades from the various governmental departments illustrating any positive or negative trends. Some departments displayed increases in computer security, instilling positive procedures and techniques, while others declined in the negative direction.<sup>52</sup>

Agency	2005 Score	2005 Grade	2004 Score	2004 Grade	2003 Score	2003 Grade	2002 Score	2002 Grade	2001 Score	2001 Grade
Agriculture	24	F	49.5	F	40	F	36	F	31	F
AID	100	A+	99	A+	70.5	C-	52	F	22	F
Commerce	67	D+	56.5	F	73.5	C-	68	D+	51	F
DoD**	38.75	F	65	D	65.5	D	38	F	40	F
Education	71	C-	76.5	C	77	C+	66	D	33	F
Energy	46.75	F	48.5	F	59.5	F	41	F	51	F
EPA	97.5	A+	84	B	74.5	C	63	D-	69	D+
GSA	92.5	A-	79.5	C+	68	B-	84	D	66	D
HHS	45.5	F	49.5	F	54	F	61	D-	43	F
DHS	33.5	F	20.5	F	34	F	--	--	--	--
HUD	67.5	D+	28	F	40	F	48	F	66	D
Interior	41.5	F	77	C+	43	F	37	F	48	F
Justice	66.5	D	82.5	B-	55.5	F	56	F	50	F
Labor	99	A+	83	B-	86.5	B	79	C+	56	F
NASA	80	B-	60	D-	60.5	D-	68	D+	70	C-
NRC	60.5	D-	88	B+	94.5	A	74	C	34	F
NSF	95	A	77.5	C+	90.5	A-	63	D-	87	B+
OPM	98	A+	72.5	C-	61.5	D-	52	F	39	F
SBA	78	C+	60	D-	71	C-	48	F	48	F
SSA	99	A+	86	B	88	B+	82	B-	79	C+
State	37.5	F	69.5	D+	39.5	F	54	F	69	D+
Transportation	71.5	C-	91.5	A-	69	D+	28	F	48	F
Treasury**	60.5	D-	68	D+	64	D	48	F	54	F
VA**	46	F	50	F	76.5	C	50	F	44	F
Government-wide Average	67.4	D+	67.3	D+	65	D	55	F	53	F

Table 7. FY2001-FY2005 Federal Computer Security Grades (FISMA)<sup>53</sup>

<sup>52</sup> Office of Management and Budget (OMB): *Fiscal Year 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, United States: OMB, Washington D.C. 2005. <http://www.whitehouse.gov/omb/> (Last accessed 25 August 2008).

<sup>53</sup> After: Fiscal Year 2005 FISMA Results.

The FY2005 FISMA results indicated a negative tendency towards network security compliance particularly from the DoD. The DoD grades from FY2001 to FY2005 indicated no improvement while other departments did improve (the largest improvement was 78%). DoD grades ranged from a minimum of 38% in FY2002 to a maximum of 65.5% in FY2003. The overall government-wide average increased from 53% in FY2001 to 67.4% by FY2005, a change of 14.4%. However, five years after FISMA was enacted, poor information security was still a widespread dilemma.<sup>54</sup>

## 2. Fiscal Year 2007 FISMA Results

The FY2007 FISMA results did not indicate any significant difference in the DoD attitude on network security compliance from the FY2005 baseline.<sup>55</sup> Only letter grades (no numerical score) were provided in the FY2007 report. Table 8 confirms that DoD network security grades (D- for FY2007 and F for FY2006) were clearly below the government-wide average of a C.

FEDERAL COMPUTER SECURITY REPORT CARD					May 2008
GOVERNMENTWIDE GRADE 2007: C (2006: C-)					
	2007	2006		2007	2006
DEPARTMENT OF JUSTICE	A+	A-	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C	D-
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	C*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	C-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	D+	F
SOCIAL SECURITY ADMINISTRATION	A+*	A	DEPARTMENT OF TRANSPORTATION	D	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	D	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	D-	F
GENERAL SERVICES ADMINISTRATION	B+	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B+	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS	F	N/A
SMALL BUSINESS ADMINISTRATION	B	B+	DEPARTMENT OF AGRICULTURE	F	F

Table 8. FY2007 Federal Computer Security Grades (FISMA) <sup>56</sup>

<sup>54</sup> Gregory Wilshusen, 3.

<sup>55</sup> Fiscal Year 2007 FISMA Results, [www.whitehouse.gov/omb](http://www.whitehouse.gov/omb) (Last accessed 25 August 2008)

<sup>56</sup> After: Fiscal Year 2007 FISMA Results.

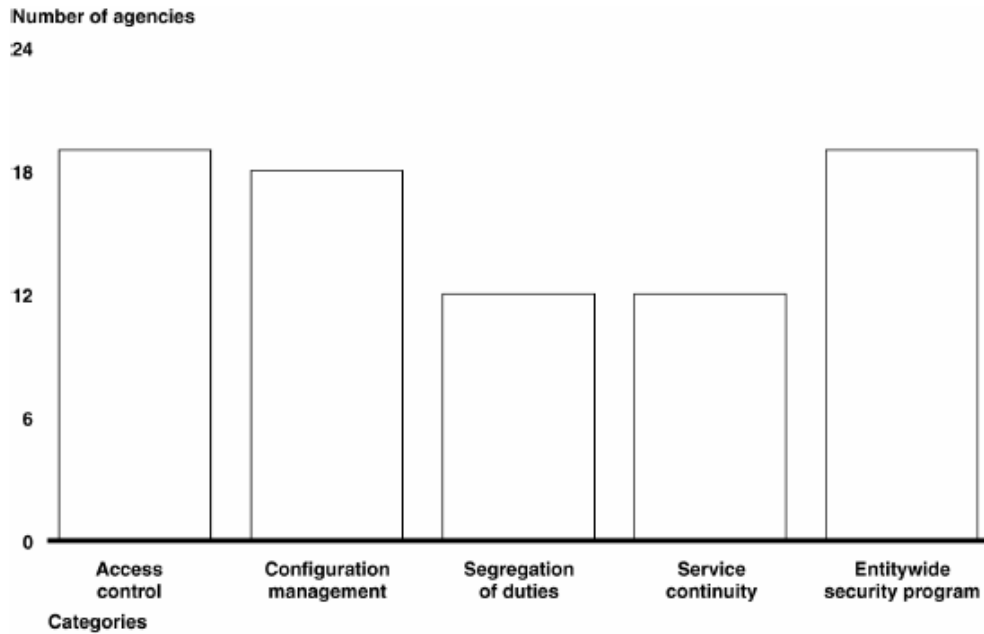
Other departments, like the Department of Justice, the Environmental Protection Agency, and Social Security Administration all showed continual improvement since FY2001. Even though the DoD incorporates and originates countless documents, doctrines, and standards to enhance network security policies and procedures for the information & knowledge managers, scores reflect a failing trend.

FISMA identifies specific government-wide weaknesses, but no specific departmental weak spots were disclosed. These persistent weaknesses are identified below:<sup>57</sup>

- Access controls, which ensure that only authorized individuals can read, alter, or delete data.
- Configuration management controls, which provide assurance that only authorized software programs, are implemented.
- Segregation of duties, which reduces the risk that one individual, can independently perform inappropriate actions without detection.
- Continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations.
- An agency-wide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented

---

<sup>57</sup> Gregory Wilshusen, 12-20.



Source: GAO analysis of agency performance and accountability reports for FY2007.

Figure 5. Number of Major Agencies Reporting Weaknesses in Control Categories<sup>58</sup>

Continuing with the weaknesses found by the FISMA reports:<sup>59</sup>

- 19 of 24 agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Control sub-categories are listed below:
  - Identify & authenticate users to prevent unauthorized access.
  - Enforce the principle of least privilege to ensure that authorized access was necessary and appropriate.
  - Establish sufficient boundary protection mechanisms,
  - Apply encryption to protect sensitive data on networks and portable devices.
  - Log, audit, and monitor security-relevant events.
  - Agencies also lacked effective controls to restrict physical access to information assets.

<sup>58</sup> After: Gregory Wilshusen, 12-20.

<sup>59</sup> Ibid.

- Agencies had developed and documented information security policies, standards, and guidelines for information security, but did not always provide specific guidance for securing critical systems.
- Security plans were not always up-to-date or complete.
- Five major agencies reported challenges in ensuring that members had received security awareness training.
- Agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.
- Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

Left on its own, only marginal improvements to any of the previously discussed weaknesses can be expected (especially true in the DoD). To improve FISMA scores, the DoD needs to begin implementing changes to the standards and policies enforced on basic users. As previously described, users (the people) are the elementary component in the grand scheme towards information infrastructure security. Revitalizing security awareness training and ensuring compliance (through a set of rigorous metrics) is one avenue of approach to enhancing network security and instilling the elements of Information Assurance throughout the DoD information infrastructure. In addition, a best IA practices framework needs to be initiated and implemented throughout DoD infrastructures/installations. The IA best practice rule set should be managed by the network managers, but carried out daily by the individual users. Non-compliance to any procedural requirement should be handled appropriately. The people need to be held accountable for their actions.

## **D. RECAP**

Whether in the civilian market or in the federal government, defending information and networks against network attacks (inside and outside) must be a cause that is readily realized by all unit members. Refinement of current security mechanisms and Information Assurance standards and procedures are the bare minimum courses of action. Actions need to be an “all-hands” effort. Chapters IV and V will analyze the existing DoD Information Assurance training standard and propose meaningful changes and recommendations that will ensure better FISMA report cards (even though the report cards are only an indicator of improved information security and dominance). Additionally, a safe-user, best practice model for user behaviors, roles and responsibilities will be presented to tackle segments of the third priority of *The National Strategy to Secure Cyberspace* (A National Cyberspace Security Awareness and Training Program) and develop a useful set of metrics that can be employed to evaluate the performance of the safe user model.

## IV. REVITALIZED INFORMATION ASSURANCE APPROACH

### A. INTRODUCTION

Many potential cyber (relating to, or involvement of, computers and networks) vulnerabilities exist because of a lack of cybersecurity awareness on the part of the computer users, system administrators, technology developers, and the chief information officers, just to name a few. Such awareness-based vulnerabilities present serious risks to critical information network infrastructures regardless of whether they currently exist, or potentially exist, within the infrastructure itself. A lack of trained personnel and the absence of widely accepted Information Assurance (IA) programs complicate any hope of reducing cyber vulnerabilities.<sup>60</sup> This chapter describes how knowledge and information managers need to enforce training standards and implement IA “best practice” rules of behavior to defeat such risks and vulnerabilities and to ensure that required infrastructures are secure.

The National Strategy to Secure Cyberspace defined several meaningful tasks toward cyberspace awareness. One cited awareness element, *Priority III: A National Cyberspace Security Awareness and Training Program* emphasized the need to increase the efficiency and compliance of cybersecurity training in Government, companies, universities, and the Nation’s computer users.<sup>61</sup> Furthermore, explicit actions of Priority III were offered to enhance the awareness, education and training of Information Assurance for all users. These explicit actions are listed below:

- Promote a comprehensive national awareness program to empower all DoD service members to secure their own parts of cyberspace.
- Foster adequate training and education programs to support the Nation’s cybersecurity needs.
- Increase the efficiency (i.e. reducing the amount of cybercrime) of existing federal cybersecurity training programs.

---

<sup>60</sup> President of the United States, *The National Strategy to Secure Cyberspace*, 4.

<sup>61</sup> *Ibid*, 37-38.

## B. IA AWARENESS TRAINING

### 1. The Current Method

The current DoD IA awareness training is conducted on a yearly basis. IA training is web-based and the overall content is sufficient, but to a certain extent elementary. The user launches the web based trainer (via NKO, AKO, or NPS for example)<sup>62</sup> and basically executes an interactive session. The course is divided among six sections (refer to Figure 6). Below are a few screenshots of the current DoD IA Training:

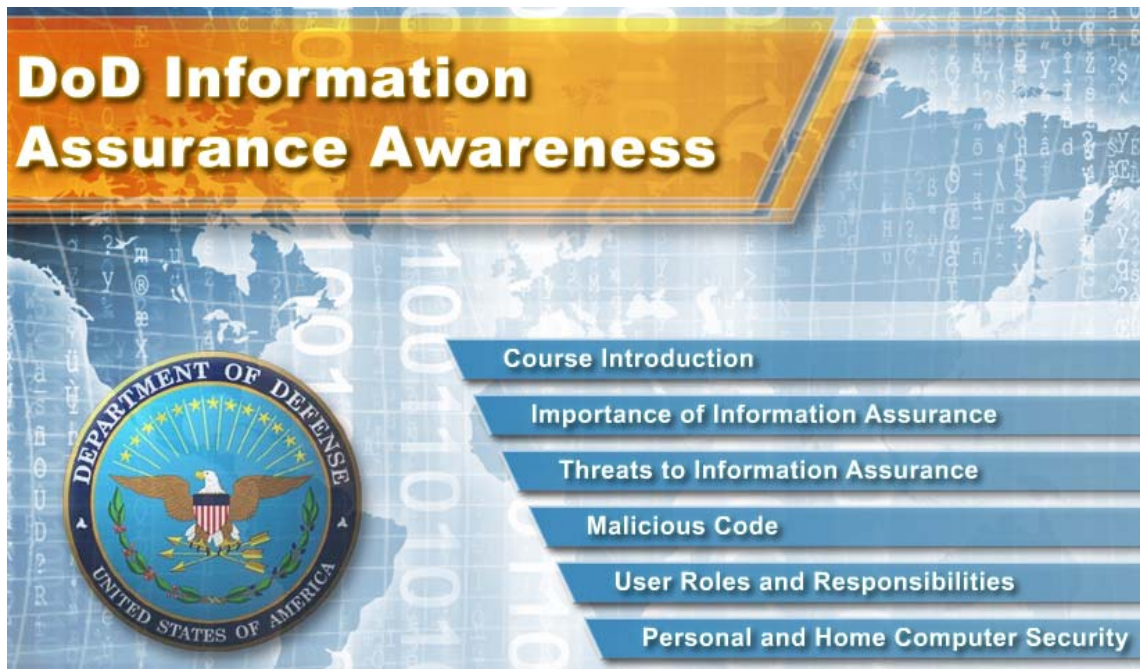


Figure 6. DoD IA Training Start-Up Page <sup>63</sup>

---

<sup>62</sup> NKO: Navy Knowledge Online. AKO: Army Knowledge Online. NPS: Naval Postgraduate School.

<sup>63</sup> DoD IA Training Course. DoD Information Assurance, *Training Notes*, Annual IA Trainer via NPS Training Site: Pappas Notes, 2008.

A sample page of the web-based trainer is illustrated in Figure 7. This particular page describes the IA Legal Requirements, *Policy and Law*, under the Importance of Information Assurance segment of the IA training.

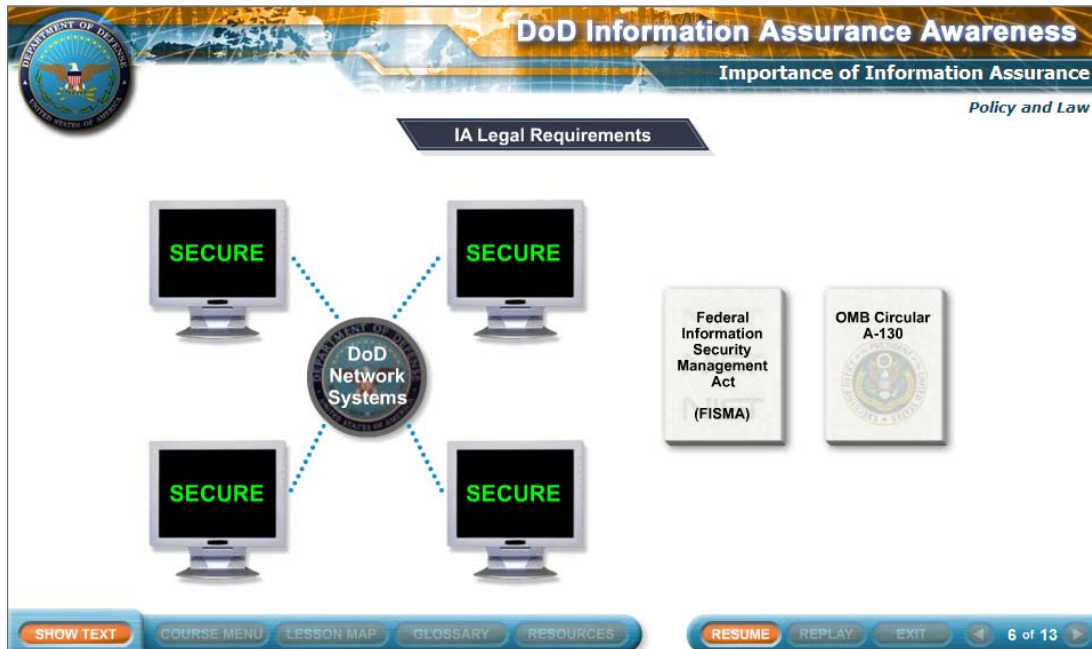


Figure 7. Sample IA Training Page <sup>64</sup>

In essence, the construct of the current IA security awareness training is only adequate towards an objective of “putting a check in the box” as users are not required to validate any level of proficiency. Upon completion of the required IA training, each user prints a certificate and IA training is then considered as sufficient and complete for the entire year. In completing training, no feedback or question & answer metrics are utilized to account if the user grasped and/or understood even minimal understanding of the content of the IA training. Other than a check on completion of the requirement, no training direct supervision is involved either. Without some form of training monitoring, the user can simply click the “next” button to advance to the next lesson and finish the training module in far less time than is allotted. By advancing as described, the user is

---

<sup>64</sup> DoD Information Assurance, *Training Notes*.

ignoring the significance of IA and displaying the exact behavior the training is trying to reduce. Finally, the time to complete the annual requirement (not to be confused with the actual time needed to complete the web-based training itself) is not a standard that is monitored or enforced by network managers. The next section proposes the changes needed to revitalize the DoD Information Assurance training program.

## **2. A New Hope**

“A New Hope,” fits well as the title to describe the necessary actions needed to incorporate a more efficient cybersecurity training mechanism. With the goal of improving existing IA policy, training and infrastructure, most of the key elements that work today will be retained and revitalized. The IA “training wheel” does not need to be reinvented if positive merits can be continued. It is recommended that the web based-trainer should remain the same in general appearance and content, but feedback, measures, and compliance need revitalization (or added in if absent in the current training). Furthermore, knowledge and information managers must, if not already procedurally in place, take charge (in a more effective manner) in the enforcement of IA training and as a result institute a standard set of IA best practices within their respective information environments. By adopting a revitalized IA proposal, the people and organization can gain a more watchful eye towards cybersecurity awareness, better understand the basic IA practices needed, and as a result assure that the value of information on their critical networks will not be compromised. A set of procedural steps describing the proposed revitalization enhancement process is as follows:

### ***a. Step 1: Incorporate Feedback and Question & Answer Criteria***

The first step towards the proposed revitalization is to expand the IA training course by integrating feedback to the current structure. The presentation and content of the existing IA training model is generally acceptable; however user feedback needs to be incorporated throughout every section to ensure that objectives and goals of the program are attained. Additionally, at the completion of the IA Training, a question and answer evaluation must be instituted before an annual IA certificate is granted. It is

recommended that individuals should pass a 10-Question proficiency examination with a minimum score of 80%, and if unsuccessful, users must retake the test until a passing score is achieved. Questions should be randomized to ensure users are not simply caching (copying) questions and answers. It is also recommended that questions be formatted as either multiple choice or True/False format; a format very recognizable with the DoD structure. Appendix A includes 25 sample questions (and associated answers) derived from the annual DoD IA training course that could effectively be used to evaluate user comprehension and knowledge gained from the revitalized Information Assurance Awareness Training. Listed below are three specific examples of sample questions from Appendix A to be used for the 10-Question proficiency examination:<sup>65</sup>

- Multiple Choice: What is the definition of Information Assurance? *Measures that protect and defend information systems by ensuring their availability, integrity, confidentiality, authentication, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.*
- True or False: Information Risk Management is a statement by management dictating the role security plays on the organization? *False, a security policy dictates this role.*
- Multiple Choice: What is a social engineering element of information assurance? *The act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.*

**b. Step 2: Increase IA Currency Requirements**

The second step towards training revitalization is to increase the currency requirement for training. Presently, IA training is conducted annually and most often the timing is based on a training requirement established for the entire organization, not by when a user first logs onto a network. The author of this investigation believes that this

---

<sup>65</sup> Questions are derived from the DoD IA Training Course. DoD Information Assurance, *Training Notes*.

standard is not adequate to assure the confidentiality, integrity and availability of the information within an infrastructure. New requirements are required that maintain the annual training requirement with additional refresher training tests required every 90 days. At a minimum, refresher tests are recommended in concert with the DoD quarterly “password change” requirement. If a user forgets or loses his/her password and a password change is initiated, a new “90-Day” IA refresher will be required as well. This will not reset a user’s “90-Day” baseline date; rather it should be viewed as an extra training session. The “90-Day” refresher requirement is based from the annual IA training date. The date of the annual IA training establishes a user’s baseline date and the “90-Day” test will progress from that established baseline date. For new personnel, the annual IA training is first established on the date the user processes into a new organization.

*c. Step 3: Time Minimum*

Step three is to put minimum time restrictions on each training slide. The user’s ability to advance to the next slide before the minimum allotted time shall be restricted to deny those that would simply game the training program. Each slide will display a time counter, indicating the time remaining until the next segment can be initiated. Additionally, feedback questions, as described in step one, shall be randomly placed throughout the lecture to ensure users are actively involved with the training instead of leisurely scrolling through the material. As observed in past IA training sessions, individuals often involve themselves with other tasks while the training is in session. By incorporating feedback and questions throughout the trainer, the user will be forced to provide feedback and answers to proceed with the trainer, and therefore pay exclusive attention to the IA training module.

*d. Step 4: “90-Day” Specifics*

Step four specially addresses the “90-Day” refresher trainer. Questions for the “90-Day” test will be just as detailed as the annual trainer, however only five questions will be utilized. Users must answer 4 of the 5 questions correctly to fulfill the

90 day requirement. If a user fails the 80% criteria, another set of five random questions will be required. Upon completion of the IA “90-Day” standard, in unison with the quarterly password change, users will be able to access the information network knowing that they have a role in safeguarding the information they use day in and day out. If, however, they repeatedly fail the “90-Day” test requirements, they are unprepared for network operations and should be denied access. The maximum number of failures for the “90-Day” refresher should be limited to five and consequently the annual requirement is therefore required.

*e. Step 5: The Consequences for Non-Compliance*

The final step is focused more for the information and knowledge managers. Information and Knowledge managers need to stress the importance of IA in the workspace and address the ramifications of poor IA procedures and how they may inflict harm within networks. Furthermore, consequences need to be enforced if individual users abuse network security practices or are non-compliant with the current standards and policies. Managers need to maintain network defense and assume the managerial role as the “first line of defense” in the struggle with information flow. Network requirements should be viewed in the same way that any other organizational standard is viewed and enforced. For example, if a user violates any network procedural requirement he/she will have to re-accomplish the annual trainings at a minimum. Additionally, the user will lose network access for a minimum of 3 duty (working) days. As for repeat offenders, users will have to re-accomplish annual training in concert with a written/oral examination administered by the respective knowledge/information manager, and lose network access for a minimum of 10 duty days. Additionally, the user will be limited to two 30-minute network sessions daily until the next annual trainer or at the discretion of the knowledge/information manager. Lastly, a list of IA discrepancies should be shared with unit commanders for possible administrative penalties.

### C. BEST PRACTICE IA TECHNIQUES

The research of this investigation discovered four sources providing “best practice” techniques towards information security. These practices ranged from the government sector to the civilian sector, all instilling methodical schemes, yet diverse stances to achieving safe user network security environments. These four selections are listed below using the parent organization(s) from which they were derived:

- *Common Risks Impeding the Adequate Protection of Government Information*, Office of Management and Budget (FISMA).<sup>66</sup>
- *Common Sense Guide to Cyber Security for Small Businesses*, Internet Security Alliance.<sup>67</sup>
- *Build Security in: Training and Awareness*, Carnegie Mellon University (Sponsored by the DHS National Cyber Security Division).<sup>68</sup>
- *Common Sense Guide to Prevention and Detection of Insider Threats*, Carnegie Mellon University and Internet Security Alliance.<sup>69</sup>

#### 1. Best Practice Source 1: Common Risks Impeding the Adequate Protection of Government Information (via FISMA)

The Office of Management and Budget, via the FISMA results, investigated the common mistakes and risks impeding the various agencies from adequately protecting critical government information. Each risk or mistake FISMA identified is associated

---

<sup>66</sup> Karen Evans, *Top 10 Risks Impeding the Adequate Protection of Government Information*, The Department of Homeland Security and the Office of Management and Budget, Washington D.C. 2007.

<http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf> (Last accessed 09 August 2008).

<sup>67</sup> Carol Woody and Larry Clinton, *Common Sense Guide to Cyber Security for Small Businesses, Recommended Actions for Information Security*. 1st ed., Carnegie Mellon University and Internet Security Alliance, 2004, 8 Mar. 2007 [http://www.us-cert.gov/reading\\_room/CSG-small-business.pdf](http://www.us-cert.gov/reading_room/CSG-small-business.pdf) (Last accessed 31 August 2008).

<sup>68</sup> Kenneth Van Wyk, *Build Security In: Training and Awareness*, Carnegie Mellon University, Pittsburgh, PA (Sponsored by Department of Homeland Security National Cyber Security Division), 2008. <https://buildsecurityin.us-cert.gov/daisy/bsi/home.html> (Last accessed 30 August 2008).

<sup>69</sup> Dawn Capelli, *Common Sense Guide to Prevention and Detection of Insider Threats, 2nd Ed*, Carnegie Mellon University CyLab, Internet Security Alliance, Pittsburgh, PA, July 2006. [www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf](http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf) (Last accessed 31 August 2008).

with a recommended best practice technique(s) to alleviate the poor computer security standards. Of the 10 common risks provided in the OMB report, six were selected for this analysis to further consider towards a DoD IA best practice rule set. Below are the six risks with their corresponding best practice techniques:<sup>70</sup>

***a. Risk 1 of 10: Security and Privacy Training is Inadequate and Poorly Aligned with the Different Roles and Responsibilities of Various Personnel***

Best Practices Techniques to Mitigate Risk 1 of 10:

- Agencies provide security and privacy training for all personnel upon hiring and at least annually. Both initial and refresher training explain acceptable rules of behavior and the consequences when rules are not followed.
- Agencies assess whether training is effective, and adapt training to address changing requirements and emerging threats.
- Agencies require personnel to sign documentation verifying they completed training, track the number of personnel trained, and consider whether training was completed when evaluating personnel performance.

***b. Risk 5 of 10: Suspicious Activities and Incidents are Not Identified and Reported in a Timely Manner***

Best Practices Techniques to Mitigate Risk 5 of 10:

- Agencies develop and implement standard operating procedures describing how to identify and report suspicious activities and incidents.
- Agencies report suspicious activities and incidents in a timely manner to mitigate harm and prevent similar incidents from re-occurring.
- Agencies configure systems to log security events and monitor the logs to detect suspicious activity.

---

<sup>70</sup> Karen Evans, 1-3.

- Agencies document lessons learned after responding to incidents and incorporate them into security and privacy awareness training accordingly.
  - Agencies route employee web traffic through approved servers to simplify the monitoring of web traffic for malicious content.
- c. *Risk 6 of 10: Audit Trails Documenting how Information is Processed are Not Appropriately Created or Reviewed***

Best Practices Technique to Mitigate Risk 6 of 10:

- Agencies log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required.

**d. *Risk 7 of 10: Inadequate Physical Security Controls***

Best Practices Technique to Mitigate Risk 7 of 10:

- Agencies regularly review procedures, at least annually, for allowing physical access to buildings and specific areas to only those who are authorized.

**e. *Risk 8 of 10: Information Security Controls are Not Adequate***

Best Practices Techniques to Mitigate Risk 8 of 10:

- Security controls are tested regularly, and at least annually, to ensure they are effective.
- Personnel who test controls work closely with, but remain separate from, the personnel administering them.
- Agencies maintain an accurate plan of action and milestones to fix security controls needing improvement.
- Agencies consider the public availability of related information as a factor when determining how to protect government information.

*f. Risk 9 of 10: Inadequate Protection of Information Accessed or Processed Remotely*

Best Practices Techniques to Mitigate Risk 9 of 10:

- Agencies maintain an audit log of information accessed or processed remotely, as appropriate.
- Agencies use privacy screens when working outside the office.

OMB identified risks covering the physical, training, procedural, and information security aspects related to network user behavior. Protecting the information and systems that the Federal government depends on is important since agencies increasingly rely on new technology. In essence, agencies are working to preserve the integrity, reliability, availability, and confidentiality of important information while maintaining their information systems. The most effective way to protect information and systems is to incorporate security into the architecture of each. The best practice techniques described above provide a few possible solutions to the many risks presented from the FISMA report to overcome computer security deficiencies.

**2. Best Practice Source 2: Common Sense Guide to Cyber Security for Small Businesses**

The Common Sense Guide presents the case that small and medium-sized businesses are not cyber-immune and have been significantly harmed by various cyber attacks in the past. No longer are large corporations and governmental agencies the only targets of opportunity.

Below are the top ten selected best practice techniques selected from *Common Sense Guide to Cyber Security for Small Business*:<sup>71</sup>

- Use Strong Passwords and Change Them Regularly
- Look Out for E-mail Attachments and Internet Download Modules
- Install, Maintain, and Apply Anti-Virus Programs
- Install and Use a Firewall

---

<sup>71</sup> Carol Woody and Larry Clinton, 3-4.

- Remove Unused Software and User Accounts; Cleanout Everything on Replaced Equipment
- Establish Physical Access Controls for all Computer Equipment
- Create Backups for Important Files, Folders, and Software
- Keep Current with Software Updates
- Implement Network Security with Access Control
- Limit Access to Sensitive and Confidential Data

The small business best practice techniques provide the user and respective managers the necessary precautions and actions needed to preserve the merit of the information within a network and the value of the network itself. The small business best practice blueprint covers procedural and informational aspects related to network user behavior.

### **3. Best Practice Source 3: Build Security in: Training and Awareness**

No best practice rule sets were selected from this source, except for a basic principle about target audiences. The Carnegie Mellon University example stressed that best practice software security training programs should plan differently for the various target audiences.<sup>72</sup> The Carnegie Mellon example targeted the senior decision makers, engineering managers, and software developers as the three choices for their target audience. To employ this model towards the DoD the three target audience choices would be: Senior Leadership (CO/XO), Information/Knowledge Managers and IT staff, and lastly the individual users.

---

<sup>72</sup> Kenneth Van Wyk, 1-3.

#### **4. Best Practice Source 4: Common Sense Guide to Prevention and Detection of Insider Threats**

The last of the best practice rule sets analyzed was Carnegie Mellon CyLab's best practice techniques to counter and help prevent insider attacks corrupt an information infrastructure. Implementation of the following 13 practices will provide an organization the defensive measures that could prevent or facilitate early detection of the many insider attacks other commercial industries have experienced.<sup>73</sup> Below are the 13 best practices for preventing insider attacks:

- Institute periodic enterprise-wide risk assessments.
- Institute periodic security awareness training for all employees.
- Enforce separation of duties and least privilege.
- Implement strict password and account management policies and practices.
- Log, monitor, and audit employee online actions.
- Use extra caution with system administrators and privileged users.
- Actively defend against malicious code.
- Use layered defense against remote attacks.
- Monitor and respond to suspicious or disruptive behavior.
- Deactivate computer access following termination.
- Collect and save data for use in investigations.
- Implement secure backup and recovery processes.
- Clearly document insider threat controls.

The Carnegie Mellon best practice techniques provide safety measures and actions required to prevent and detect insider threats from within an installation. Although these techniques are labeled common sense, they are at times overlooked or neglected, thus needing reemphasis and readdressing. The first line of defense from insider threats is the employees themselves. Security awareness must be instilled in the organization so that all employees understand the need for policies, procedures, and

---

<sup>73</sup> Dawn Capelli, 15-16.

physical controls. Once again we see that the insider best practice techniques encompass the procedural and information security aspects related to network user behaviors.

## **5. Information Assurance Best Practice Rule Set**

Based on the previous four examples presented above, a best practice rule set was compiled and categorized into four main sub-categories: Physical, Training, Informational, and Procedural-User. Within each sub category, the best practices are ranked by priority in descending order allowing the network manager to refer to specific categories and select best practices to incorporate them into their respective networks. Listed below are the categorized IA Best Practice techniques with corresponding rankings within each sub-category:

### ***a. Physical Rule Set***

Physical best practices techniques pertain to the measures needed to prevent or deter attackers from accessing a facility or resource.

- Establish Physical Access Controls for all Computer Equipment
- Use extra caution with system administrators and privileged users.
- Review procedures, at least annually, for allowing physical access to buildings and specific areas to only those who are authorized.

### ***b. Training Rule Set***

Training best practice techniques pertain to the measures needed to ensure proper and effective training resources are established and/or enforced to protect a facility, network or the information it possesses.

- Provide security training for all personnel upon hiring and at least annually.  
Both initial and refresher training explain acceptable rules of behavior and the consequences when rules are not followed.
- Assess whether training is effective, and adapt training to address changing requirements and emerging threats.

- Require personnel to sign documentation verifying they completed training, track the number of personnel trained, and consider whether training was completed when evaluating personnel performance.

*c. Informational Rule Set*

Informational best practice techniques pertain to the measures needed to protect the value of the information within a given infrastructure or installation.

- Consider the public availability of related information as a factor when determining how to protect government information.
- Clearly document insider threat controls.
- Log all computer-readable data extracts from databases holding sensitive information.
- Maintain an audit log of information accessed or processed remotely, as appropriate.

*d. Procedural*

Procedural best practice techniques pertain to the measures needed to protect a network through the policies, standards, and procedures imposed daily with respect to user roles, responsibilities and behaviors in order to maintain safe working network environments.

- Security controls are tested regularly, and at least annually, to ensure they are effective.
- Institute periodic enterprise-wide risk assessments.
- Use Strong Passwords and Change Them Regularly.
- Install, Maintain, and Apply Anti-Virus Programs.
- Install and Use a Firewall.
- Implement secure backup and recovery processes.
- Enforce separation of duties and least privilege.
- Report suspicious activities and incidents in a timely manner to mitigate harm and prevent similar incidents from re-occurring.

- Monitor and respond to suspicious or disruptive behavior.
- Remove Unused Software and User Accounts; Cleanout Everything on Replaced Equipment.

The author recommends knowledge and information managers integrate this compiled set of best practice rule into their respective installation's security plans to preserve and maintain a safe working network environment. By dividing the rules into four main categories, managers can pick and chose particular rules from individual best practice categories or select entire best practice rule sets to incorporate in their respective networks or security plans. Either way, managers and/or users now possess a rigid set of IA best practice rules to comply with in order to practice and execute first-class computer-security work ethics.

#### **D. RECAP**

Chapter IV of this thesis explored the changes needed to the current DoD Information Assurance training program and proposed a revitalized approach to strengthen the measures needed to battle the information management dilemma. The later half of the Chapter IV introduced the various best practices techniques found in the government and commercial industry. Those best practice techniques were further divided into four categories covering any DoD and commercial guidelines for network security and protection. In Chapter V, the IA best practice techniques along with the revitalized IA training approach will be evaluated and validated for its efficiency and effectiveness for future operations. Finally, Chapter V will introduce recommendations and improvements for any shortcomings determined.

## **V. ANALYSIS, RECOMMENDATIONS AND EVALUATION METRICS**

### **A. INTRODUCTION**

The struggle for information management is a battle that cannot be won overnight, or by way of part-time support. Similar to the “long war” (the Global War on Terror) we are currently engaged in with terrorist networks, the information dominance effort needs to be an “all-hands” endeavor to overcome the information management dilemma for the long haul. Thus far in this investigation, many doctrines, standards and policies at various levels in the U.S. Government were analyzed in Chapter II, painting a clear picture and expressing in great detail the immense challenges information management encompasses. Over the past decade, words like “network”, “internet” and “cyberspace” have become a common part of many people’s vocabulary and lives.

In Chapter III, the topic of internet dependency was discussed, illustrating that people, especially the citizens of the United States, basically require the full use of the internet to fulfill many everyday needs. Today, the network, internet, and cyberspace enables people to communicate and accomplish everyday business, purchase movie/airline tickets, read newspapers articles or attain assorted bits of information in a fraction of the time that previous research efforts required. Unfortunately, cyber-attackers, both internal and external, have also used these very same three words (network, internet, and cyberspace) to corrupt our information and information infrastructures or to capture our information in raw form for exploitation purpose. Furthermore, Chapter III reported on the ‘poor’ federal computer security grades (FISMA), indicating that a recourse was clearly needed.

Chapter IV explored two viable methods to alleviate these poor grades and counter the information management dilemma via the people-organizational route (revitalized training and incorporation of “best practice” lessons). Rather than address the managers of our information sources and information management systems, this investigation chose instead the people-organization element as the target of opportunity

with the largest potential return. The first method presented in this investigative study was to revitalize the Information Assurance training program while the second method set about to incorporate an IA “best practice” technique rule set to help deal with the ever-growing challenges of information management. Both solutions were discussed in detail in Chapter IV. Chapter V builds on that previous information by seeking to illustrate the key features of the four best practice publications analyzed and to both establish preferred IA methods and formulate recommendations. Furthermore, Chapter V will establish a set of performance metrics to evaluate the two possible solutions and introduce any future changes that might emerge or re-attack any related vectors dealing with opposition to any deficiencies or shortcomings if and when they should appear.

## **B. KEY FEATURES**

### **1. Publications**

Many publications were examined in this Information Assurance practice analysis. Most were informative, most were also somewhat redundant, but the majority of all the publications had the primary goal of setting standards and policies to keep important networks safe and protected. Unfortunately, the same majority of the publications did not begin to address the important topic of establishing acceptable and valuable user perspectives towards actually achieving network security. Instead, most were designed for the designated authorities or information managers placed in charge of maintaining the information flow within the information infrastructure. In the author’s opinion, a view restricted to only the manager’s perspective dooms any effort towards improved network assurance from the very beginning. True and lasting improved network assurance relies on enforcing a set of proven techniques and modifying unacceptable user behavior, policy, and procedure through informed Information Technology (IT) management and training programs.

### **2. Information Assurance Training**

The revitalized approach (described earlier in Chapter IV) to the current IA structure prescribed many procedural changes and proposals intended to make certain

that IA training was not just another mandatory training exercise. Furthermore, the critical information gained via the trainer, even if effective in design and scope, would often be forgotten about or ignored until the next year's training session – because of the time frames currently used (i.e. annually). The revitalized approach introduced the necessary steps to revive and strengthen training modules. Key features of the proposed revitalized IA training model mainly center on the user and organizational involvement, both of which are essential elements to program success. The top three features from the revitalized training approach are described below:

***a. Feature 1: Comprehension of IA Knowledge***

Past training models did not require feedback or Question and Answer sessions. The revitalized approach removes this shortcoming by requiring 10-Question Proficiency testing to receive an IA Training certificate. Additionally, feedback questions are interjected throughout the annual training to ensure the trainee is actively engaged with the training session and grasping the material content. The “90-Day” refresher test consists of 5 questions, vice the 10 questions for the annual. Minimum score for both annual and quarterly testing is recommended as 80%.

***b. Feature 2: Currency Requirements***

Increasing the currency requirements of the trainee will help to solidify the trainee's knowledge gained from the IA trainer and sustain a nearly continuous level of IA proficiency. “90-Day” refresher tests will restore the user knowledge base, stressing the day-to-day importance of IA in the workspace. The proposed “90-Day” refreshers will occur in concert with required quarterly password changes. In a given year, a user will complete one annual trainer and three refreshers, at a minimum. Additional testing may occur, at the discretion of the knowledge/information manager.

***c. Feature 3: Consequences for Violations***

Individuals who violate any network procedural standards must face the necessary consequences and penalties. Violators will re-accomplish the annual training requirement & proficiency testing and lose their network privileges for 3 consecutive

workdays, minimum. Repeat offenders will re-accomplish the annual training & testing, complete a verbal/oral test with the knowledge/information manager, lose network privileges for 10 days minimum and be limited to two 30 minute network sessions daily (to get mail and for organizational situational awareness information).

### **3. Information Assurance Best Practice Rule Set**

The best practice rule set for Information Assurance is a compilation of the various techniques found in the government and civilian sectors. The IA best practices summary presented at the end of Chapter IV are identified as designs that will ensure that the knowledge/information manager can accomplish Information Management requirements. Those requirements include meeting specific security goals and objectives that ensure that essential actions are employed by all authorized network users and to safeguard the information within his/her respective installation/infrastructure. Inherently, risks and vulnerabilities will exist no matter what standards are implemented. Best practices are valuable and essential because they reduce these risks to manageable and sustainable levels. The compiled IA best practice rule set was divided into 4 groupings: Physical, Training, Informational, and Procedural. These four groups are the key features of the recommended IA best practices techniques listed below:

#### ***a. Feature 1: Physical Rule Set***

Physical best practices techniques are intended to prevent or deter attackers from accessing a facility or critical information resource. Physical rules must be established and executed to further protect the confines, resources and the facility from potentially hazardous external and insider threats. Procedures relating to physical access points should be reviewed periodically and understood by all network users. Additional vigilance must be devoted by informed users to contribute to the goal of keeping the facility and information safe.

#### ***b. Feature 2: Training Rule Set***

Training best practice techniques are intended to ensure proper and effective training resources are established and enforced to protect a facility, network or

the information it possesses. Therefore, all users in an organization must understand that training policies and procedures exist, that there is good reason for why they exist, that they must be strictly enforced – no exceptions, and that there can be serious consequences for any infractions. Each user needs to be aware of the organizations network information management security policies and the procedural elements related to detecting violations, securing vulnerabilities and of reporting incidents. Training must not be looked at lightly. All users shall adhere to the rigid training requirements annually and quarterly.

***c. Feature 3: Informational Rule Set***

Informational best practice techniques intend to protect the value of the information within a given infrastructure or installation. Periodic monitoring and auditing provides both the network manager and system user the opportunity to discover and investigate suspicious behavior, both internal and external, and to react before serious consequences may ensue.

***d. Feature 4: Procedural Rule Set***

Procedural best practice techniques, when properly executed, provide a protected network through policies, standards, and procedures put in place to maintain safe working network environments. Strict user compliance to the best practice rules and treating them as mandatory processes, checklists and procedures will solidify good practices and habits throughout an installation. Standards policies and procedures will ultimately become everyday common knowledge if the best practice rules are applied and enforced daily.

**C. RECOMMENDATIONS**

**1. Authorize the Revitalized Approach**

The author of this investigation recommends that instituting the proposed revitalized approach toward Information Assurance needs to be implemented now. By postponing the revitalized approach, more risks and vulnerabilities become apparent,

exposing increased occurrences of holes and weakness in the network infrastructure, allowing even more information, and the network infrastructure itself, to possibly be compromised.

From the P-O aspect, the largest gain from the current dismal report cards for IA security effectiveness is expected to come about as a result of changing user behavior. Training is one of the time-proven methods that will instill a better understanding and awareness of the potential harm people may inflict within an infrastructure or installation. Increasing the currency of the training, implementing proficiency tests, and enforcing the consequences will ultimately serve to sustain and enhance the user's IA frame of mind. Enhancement includes understanding the user roles/responsibilities for identifying potential risks, accessing those risks, and taking action on those risks to thwart any impending harm from penetrating the information environment.

## **2. Implement IA Best Practice Rule Set**

The author of this investigation also recommends that enforcing the IA best practice rule set in unison with the training is needed to improve and reinforce the IA infrastructure. From the P-O perspective, the network users (people) are the basic roots and foundation of an efficient security program and in order to demonstrate effectiveness, the people need to exhibit 100% compliance towards the IA best practice rules. Machines and computers only do what people tell them, or program them, to do. Advertising and enforcing the IA best practice rule set can only help promote the need for strong procedures and policies for total compliance. By displaying the rules on posters, billboards or placards throughout an installation, rules can be frequently reviewed, thus battling the information dilemma by all fronts. Additionally, dividing the best practice rule set into 4 main sub-categories allows the manager or user to pick and chose specific rules from any subset. For example, a user/manager can pick single best practice rules from the Physical and/or Training best practice rule set and then incorporate them into his/her daily practice. Additionally, the user/manager can also select a complete rule set (like Procedural) to then incorporate into his/her daily practice as conditions require.

Utilizing both methods (training and best practice methods) can help reduce the amount of incidents. Additionally, both of these methods can decrease the amount of information lost to an incident as well as the possible financial losses. From the FBI's 2007 Internet Crime Report, incidents cost the government \$198,440,000 in 2006 and \$239,090,000 in 2007.<sup>74</sup> This is a far cry from the 2001 figures of \$17,800,000. To get back to acceptable & manageable trends, or to significantly reduce the damaging financial impact on an organization, security measures must be instilled now.

#### **D. SAFE-USER MODEL**

The Safe-User Model is the combination of both recommended methods (revitalized IA training and the IA best practice rule set) in order to provide the People and the Organization the necessary tools and resources to therefore achieve Safe-User awareness, behaviors and habit patterns. The Safe-User Model illustrates that full integration of both techniques is the optimal approach for success. Below, training is denoted as Yellow and the best practice rules are denoted Blue. Utilizing both methods completely and in unison will allow both input circles to merge together (go green) and ultimately infuse solid IA principles throughout an installation or infrastructure. By implementing both inputs of the Safe-User Model, knowledge & information managers will eventually reach the safe "green" zone, thus overcoming the P-O influence with respect to computer/information security.

---

<sup>74</sup> Internet Crime Complaint Center (IC<sup>3</sup>), *2007 Internet Crime Report*, 3.

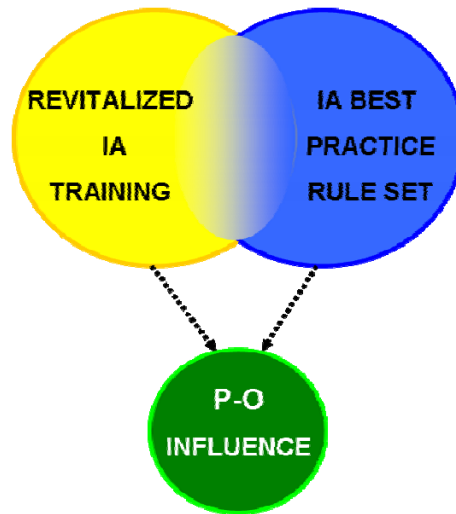


Figure 8. Safe-User Model

#### **E. VALIDATION OF THE RECOMMENDATIONS**

From the recommendations described above, validation measures need to be devised to measure and track if the safe-user model (revitalized annual training complemented with wholesale adoption of best practice methods) discussed are properly functioning. These validation metrics are used to measure the effectiveness of the IA training and the implementation procedure of the best practice IA rule set. The metrics are designed to be instituted on a yearly basis.

To clarify, the compliance measures, similar to the FISMA reports, need to evaluate the training and best practices methods on a yearly basis in order to determine if issues need to be readdressed or re-attacked to achieve information dominance goals and expectations. Of note, year one measurement results will act as the baseline results for validation for all subsequent years, due to the fact that no measures, except for compliance, may have been measured in years past.

## **1. Validation Metrics**

The overall goal of the validation metrics is to monitor the trends (positive or negative) in computer security compliance with respect to Information Assurance. Without this data, there is no feedback available on effectiveness. The following metrics (refer to Table 8) are proposed in order to validate and measure the effectiveness of the revitalized training mechanism and IA best practice techniques.

The evaluation criteria for each of these validation metrics are numerically based. Quantitative data is recommended to support tracking the various categories listed and the results will be scorecard documented on a yearly basis. Year one results, as mentioned above, will establish the baseline figures for follow-on years to be further compared and contrasted with. Categories range from the number of incidents, average days to complete either trainer, number of violators, to the commonly violated best practice rules. All measures are to be reported at the organization level, and then to the installations parent command and ultimately rolled-up and disclosed to the Office and Management and Budget via the annual FISMA report.

The validation metrics will test all groups associated with the DoD and the various governmental agencies. This includes military personnel, civilian employees and government contractors. For the “all-hands” effort to be successful towards improving and maintaining computer security, no group will be left untested. No exceptions.

Below, Table 8 displays the metrics to be used on a yearly basis to measure the Information Assurance performance levels from one year to the next.

Metrics of Validation			
C A T E G O R Y		200X	200Y
Information Assurance Trainer	<b>NUMBER OF:</b>		
	Personnel in command		
	Personnel Trained		
	Incidents Reported <i>Total</i>		
	<i>Yearly</i>		
	<i>Monthly</i>		
	<i>Weekly</i>		
	Users Who Completed Training		
	<i>Within 3 days</i>		
	<i>4 - 7 days</i>		
	<i>Over 7 days</i>		
	Users Who Failed the Annual Test on First Attempt		
	Violators		
	Repeat Violators		
	Users Exceeding 5 Failures on Refresher		
	Month With Most No. of Incidents		
	<b>AVERAGE:</b>		
	Score of Annual IA Test		
	Attempts to Complete Annual IA Trainer		
	Attempts to Complete Refresher Test		
	Time in Minutes to Complete Annual Trainer		
Best Practice Rules	No. of Users in Violation of Best Practice Rule Set		
	No. of Incidents Reported <i>Total</i>		
	<i>Yearly</i>		
	<i>Monthly</i>		
	<i>Weekly</i>		
	Quarter With Most No. of Incidents		
	Are Best Practice Rule Sets Openly Displayed ( YES or NO)		
	Best Practice Rules Commonly Violated		
	***Separate Report to specify Rule No. and # of Times violated		

Table 9. Metrics for Validation

For example, if a command reported 14 incidents in the year 2007 and then reported 9 incidents in 2008, the metrics report shows a negative trend for incidents. This is good. However, if 16 incidents were then reported for 2009, the manager and command leadership would become aware of this rising trend and therefore look for remedies to neutralize the increase. Additionally, these metrics, along with all other installations, would be compiled and critically examined to determine if changes to the IA training or IA best practices are overlooking any aspect with respect to Information Assurance. Perhaps, the proposed metrics themselves would evolve over time into even better indicators and thru usage and review collapse to a more optimal list than those chosen for IA program startup.

## **2. Proposed Acceptance Criteria**

For IA training to be effective, no users should exceed 7 days for completion of the training program. As the initial year progresses, the results for violations and incidents should see steady decreases from start-up values. Next, average annual test results should aim for an average grade of 90%, well above the 80% minimum threshold in order to ensure threshold level proficiencies. Additionally, the average number of attempts for completion should strive to be as close to one (1) as possible. For best practice metrics, users in violation and incidents should again see steady decreases. If increases are measured, increasing consequences and more stringent enforcement of the best practice rule set is required via managers and re-vectoring may be required. Finally, tracking the best practice rules commonly violated leads to a need for supplemental tracking reports and/or supplemental training requirements. Supplemental tracking reports will state which best practice rule was violated with the associated number of violations. Additionally, the remediation actions employed by the manager should be noted and assessed if positive outcomes were achieved. The manager would therefore track all violations/incidents, describe the remediation action employed, and document if the violator or incident was resolved in a timely manner. Reports would then be submitted to the installations parent command and ultimately rolled-up and disclosed to the Office and Management and Budget via the annual FISMA report.

## **F. POSSIBLE SHORTCOMINGS**

One possible shortcoming is the adequacy of the pool of available questions. If the question bank remains constant, users will eventually memorize the answers. If the requirements change, then the existing pool of questions may be out-dated. Changing the verbiage of the questions is needed to infuse fundamentals are tested not memorization skills and to ensure relevancy. Another possible shortcoming is if the senior leadership does not fully support the revitalized IA training changes and the “90-Day” refresher tests. In this case, command leadership must understand that poor practices within their commands could spawn risks to other installation and create a far more problem than intended. Commands need to understand that information security is an “all hands” effort, not a singular effort. Third, if consequences are not changing the bad habits of those repeat violators, escalation will be required. One solution may be to revoke all network privileges and force extra duty days and criminal prosecution. Only under direct supervision may the ‘repeat’ repeat offender be allowed to check official work related emails. Bottom Line: Because of the potential consequence, network security violations should be viewed in the same light as all other legal or procedural standard practices.

## **G. RECAP**

As the internet continues to grow, so do the associated risks and vulnerabilities. Safe-User models and measures, like improved training standards and best practice techniques, are good beginnings, but performance metrics and evaluations need to be incorporated to further counteract the actions of internal and external threats. Chapter V provided recommendations toward information/computer security using the two methods described in Chapter IV with respect to the P-O aspect. The Safe-User model illustrated how both IA elements are needed in order to overcome the P-O influence with respect to computer/information security.

Additionally, validation standards of the revitalized approach to IA training and the IA best practice rule sets were introduced for validation purposes. The metrics format presented allows for progress to be measured on a yearly basis. Furthermore, exploring

possible re-attack vectors may be needed if shortcomings arise. Finally, these possible shortcomings were discussed and possible means to correct the issues were presented. To conclude, Chapter VI provides conclusions and recommendations for future areas of research and suggestions to counter any other possible shortcomings resulting from the described Safe-User model.

The people are the root for overall success. Effectively training the people, enforcing best practices in their daily routine, and implementing strict consequences will in due course convince the people and organization to become cyber advocates against cyber crimes and threats.

THIS PAGE INTENTIONALLY LEFT BLANK

## VI. CONCLUSION

### A. SUMMARY

This investigation researched and analyzed an excessive amount of documents and publications regarding network security, information security, and information assurance. Resources ranged from the government sector to the civilian. This analysis concluded that the vast amount of knowledge available is not particularly directed towards the user roles, responsibilities and behaviors. Instead, the majority is “top level” and intended for the knowledge or information managers who maintain and preserve the critical flow of information over the rapidly expanding information networks. Guidance and strategic goals for network security were delineated from The President’s *National Strategy to Secure Cyberspace*, as this thesis paid particular attention to engage the security awareness and training program dilemma with respect to the people-organizational aspect.

The analysis then explored the people’s (the user) resounding dependency of the internet to communicate and attain information. The value of information cannot be overlooked or underestimated. Speed, accuracy, usability, relevance and content are a few of the information quality characteristics desired by most.<sup>75</sup> Next, the analysis examined the surprisingly poor results of OMB’s annual FISMA report, denoting the major flaws and discrepancies found throughout the federal government. Potential for improving computer security was evident and attainable if properly addressed. Computer and information security has, is and will be a major concern for any installation or infrastructure, civilian or governmental.

This investigation then brainstormed various means and methods to overcome the poor FISMA security grades. The selected courses of action ultimately designated the people and organizational procedure aspect as the target of opportunity utilizing a

---

<sup>75</sup> Joint Publication (JP) 3-13: *Information Operations*, I-3.

“bottom up” approach. The findings determined that current Information Assurance training standards needed to be revitalized in conjunction with the establishment an IA best practice rules set to incorporate through the DoD.

The investigation then analyzed the two selected methods (a revitalized IA training approach and an IA best practice rules set) and thus recommended that both methods need to be implemented sooner rather than later, with the hope of opposing any cyber risks or vulnerabilities that an information infrastructure may have encountered. These two recommended methods are the primary inputs for the Safe-User model introduced in Chapter V. Next, the analysis evaluated and validated the efficiency and effectiveness for both the IA best practice rules set and the revitalized IA training approach. Candidate validation metrics were then developed to further justify that the two proposed methods need to be fully integrated in all DoD installations security policies & plans to enhance information management and augment network security.

## **B. SUGGESTIONS FOR FUTURE RESEARCH**

### **1. Certification and Accreditation**

There needs to be research conducted to examine the best way of certifying and accrediting the revitalized IA training approach and IA best practice rules set. The results of such a research project would allow for the two proposed methods to be further executed and tested in order to determine if the DoD does indeed need refinement in the IA training department.

### **2. Develop Measures**

Develop measures of effectiveness and performance to quantify that the IA revitalized approach and the IA best practice rule set can provide the necessary levels of assurance.

### **3. Evaluate the Validation**

Develop a pre-evaluation metrics prior to the first year validation results of the revitalized IA training approach and IA best practice rules set. Rather than waiting one year to establish the baseline figures, develop a quarterly-based investigation to provide threshold values for the yearly validation assessments.

### **4. OPSEC Model**

Develop a similar model to further enhance and improve user and organizational awareness towards understanding the magnitude and significance of Operations Security (OPSEC) in mission critical operations.

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX      IA TRAINING SAMPLE QUESTIONS

The following list provides the 25 sample questions, for both annual and refresher tests, to be incorporated into the revitalized Information Assurance Awareness Training. Source data for the questions are derived from the annual DoD IA Trainer<sup>76</sup> and the CISSP All in One Handbook.<sup>77</sup> The format of the questions will be either multiple choice or True/False.

- 1) Multiple Choice: What is the definition of Information Assurance? *Measures that protect and defend information systems by ensuring their availability, integrity, confidentiality, authentication, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.*
- 2) Multiple Choice: What does the acronym C.I.A stand for with respect to information Assurance? *Confidentiality, Integrity, and Availability.*
- 3) True or False: INFOCON 5 is described as Maximum Readiness/Significant impact of system availability? *Answer is False, INFOCON 1 is described above.*
- 4) Multiple Choice: What document requires government employees and contractors to undergo periodic computer security training? *FISMA (Federal Information Security Management Act).*
- 5) Multiple Choice: What is the common method used to inject malicious code into an information infrastructure? *Email.*
- 6) Multiple Choice: What are examples of malicious code? *Virus, Worm, and Trojan Horses, and logic bombs are examples of malicious code.*
- 7) True of False: Only network managers are liable in enforcing Information Assurance? *Every user is responsible.*
- 8) Multiple Choice: What is a Denial of Service? *Any action, or series of actions, that prevents a system or its resources, from functioning in accordance with its intended purpose.*

---

<sup>76</sup> DoD Information Assurance, *Training Notes*.

<sup>77</sup> Shon Harris, Certified Information Systems Security Professional (CISSP): *All in One Exam Guide: Third Edition*. New York. 2005.

- 9) Multiple Choice: Define Threat? *Any potential danger to information or systems?*
- 10) Multiple Choice: Define Vulnerability? *A software, hardware, or procedural weakness that may provide an attacker the open door he/she is looking for to enter a computer or network and have unauthorized access to resources with the environment.*
- 11) Multiple Choice: Define Risk? *The likelihood of a threat agent taking advantage of a vulnerability. Also described as the loss potential, or probability, that a threat will exploit a vulnerability.*
- 12) Multiple Choice: Define Exposure? *An instance of being exposed to losses from a threat.*
- 13) True or False: The Critical Infrastructure Protection (CIP) includes Energy, Water, Banking, Information Technology & Telecommunication, Emergency Services and Transportation & Border Security? *True.*
- 14) Multiple Choice: What is confidentiality? *A security principle that works to ensure that information is not disclosed to unauthorized subjects.*
- 15) Multiple Choice: What is integrity? *A security principle that makes sure that information and systems are not modified maliciously or accidentally.*
- 16) Multiple Choice: What is availability? *The reliability and accessibility of data and resources to authorized individuals in a timely manner.*
- 17) Multiple Choice: What is more dangerous, an insider/internal threat or outsider/external threat? *Insider/internal threat.*
- 18) Multiple Choice: From the two human threat categories (insider/internal or outsider/external), who causes harm by lack of training/awareness? *Insider/internal threat.*
- 19) Multiple Choice: From the two human threat categories (insider/internal or outsider/external), who utilizes sophisticated software to identify a systems security weaknesses? *Outsider/external threat.*
- 20) Multiple Choice: What is an attack? *An attempt to bypass security controls in a system with the mission of using that system or compromising it.*
- 21) Multiple Choice: What is a social engineering element of information assurance? *The act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.*

- 22) Multiple Choice: What is another name for a countermeasure? *Safeguard.*
- 23) Multiple Choice: What ensures that no single person has total control over an activity or task? *Separation of duties.*
- 24) True or False: Information Risk Management is a statement by management dictating the role security plays on the organization? *False, a security policy dictates this role.*
- 25) True or False: By completing this training, you have a better understanding of Information Assurance and the roles and responsibilities the user needs to demonstrate? *Hopefully True.*

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- Air Force Cyberspace Command website: <http://www.afcyber.af.mil> (Last accessed 05 September 2008).
- Air Force Doctrine Document 2-5: *Information Operations*. United States: Department of Defense, Washington D.C. 2005.
- Arquilla, John and Doug Borer. *Information Strategy and Warfare*. New York. 2007.
- Bowen, Pauline, Joan Hash, and Marianne Swanson. NIST (National Institute of Standards and Technology) Special Publication 800-18, *Information Security: Guide for Developing Security Plans for Federal Information Systems*, United States: Department of Commerce, Gaithersburg, MD, 2006.
- Cappelli, Dawn. *Common Sense Guide to Prevention and Detection of Insider Threats, 2nd Ed*, Carnegie Mellon University CyLab, Internet Security Alliance, Pittsburgh, PA, 2006.  
[www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf](http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf) (Last accessed 31 August 2008)
- CNSS (Committee on National Security Systems) Instruction 4009: *National Information Assurance Glossary*. The National Security Agency, Ft. Meade, MD, 2003.
- CJCSM (Chairman, Joint Chiefs of Staff of Staff Manual) 6510.01, *Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND)*, United States: Department of Defense, Washington D.C. 2005.
- Computer Security Institute (CSI) and the Federal Bureau of Investigation, *CSI/FBI Computer Crime and Security Survey*, United States: Department of Justice, Washington D.C. 2005. <http://www.fbi.gov/page2/july05/cyber072505.htm> (Last accessed 15 August 2008).
- DCID 6/3, Director of Central Intelligence Directive 6/3: *Protecting Sensitive Compartmented Information (SCI) within Information Systems Manual*. 2000.
- Department of Defense Cyber Crime Center (DC3) website: <http://www.dc3.mil> (Last accessed 22 August 2008).
- Department of Homeland Security, *National Infrastructure Protection Plan: Risk Management Framework*, United States: Department of Homeland Security, Washington D.C. 2008.

Department of Homeland Security (DHS) National Cyber Security Division website:  
[http://www.dhs.gov/xabout/structure/editorial\\_0839.shtm](http://www.dhs.gov/xabout/structure/editorial_0839.shtm) (Last accessed 22 August 2008).

DoD Instruction (DODI) 5200.40: *Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*. United States: Department of Defense, Washington D.C. 1997.

DoD Directive 8500.01E: *Information Assurance (IA)*. United States: Department of Defense, Washington D.C. 2007.

DoD Directive 8500.2: *Information Assurance (IA) Implementation*. United States: Department of Defense, Washington D.C. 2003.

DoD Directive 8523.01: *Communications Security (COMSEC)*. United States: Department of Defense, Washington D.C. 2008.

*DODD 8530.1: Computer Network Defense*. United States: Department of Defense, Washington D.C. 2002. <http://iase.disa.mil/policy.html> (Last accessed 04 June 2008).

*DODI 8530.2: Support to Computer Network Defense (CND)*. United States: Department of Defense, Washington D.C. 2002. <http://iase.disa.mil/policy.html> (Last accessed 06 June 2008).

DoD Information Assurance, *Training Notes*, Annual IA Trainer via NPS Training Site, Pappas Notes, 2008.

Evans, Karen. *Top 10 Risks Impeding the Adequate Protection of Government Information*, The Department of Homeland Security and the Office of Management and Budget, Washington D.C. 2007.  
<http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf> (Last accessed 09 August 2008).

Federal Bureau of Investigation (FBI) website:  
<http://www.fbi.gov/cyberinvest/cyberhome.htm> (Last accessed 15 August 2008).

FIPS Pub-199, Federal Information Processing Standards Publication: *Standards for Security Categorization of Federal Information and Information Systems*, United States: Department of Commerce, Gaithersburg, MD. 2004.

Gaudin, Sharon. "Study Highlights Insider Threats," *Information Week*, 25 August 2006.  
<http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=192300421> (Last accessed 05 September 2008).

Harris, Shon. Certified Information Systems Security Professional (CISSP): *All in One Exam Guide: Third Edition*. New York. 2005.

IBM Report. "Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005," *IBM News*. 4 Aug. 2005.  
[http://www.ibm.com/news/ie/en/2005/08/ie\\_en\\_news\\_20050804.html](http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html) (Last accessed 15 May 2008).

*Information Operations Roadmap* (DECLASSIFIED), Oct 30, 2003.  
<http://freegovinfo.info/node/913> (Last accessed 01 September 2008).

Internet Crime Complaint Center (IC<sup>3</sup>), *2007 Internet Crime Report*, National White Collar Crime Center: Federal Bureau of Investigation (FBI). Washington D.C. 2007. [http://www.nw3c.org/research/site\\_files.cfm?mode=p](http://www.nw3c.org/research/site_files.cfm?mode=p)  
(Last accessed 05 September 2008).

Internet Growth graphic found on Wikipedia search on Internet Growth by Country.  
[http://en.wikipedia.org/wiki/List\\_of\\_countries\\_by\\_number\\_of\\_Internet\\_users](http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users)  
(Last accessed 09 August 2008).

Internet Users in the World Growth 1995-2010 figure found on  
<http://www.allaboutmarketresearch.com/internet.htm> (Last accessed 29 May 2008).

Johnson III, Clay, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, United States: Office of Management and Budget, Washington D.C. 2007.  
[www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf](http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf) (Last assessed 03 September 2008).

Joint Publication (JP) 1-02: *Department of Defense (DoD) Dictionary of Military and Associated Terms*. United States: Chairman, Joint Chiefs of Staff, Washington D.C. 2001 (as amended through 04 March, 2008).

Joint Publication (JP) 3-13: *Joint Doctrine for Information Operations*. United States: Chairman, Joint Chiefs of Staff, Washington D.C. 2006.

Joint Publication (JP) 3-54: *Joint Doctrine for Operations Security (OPSEC)*. United States: Chairman, Joint Chiefs of Staff, Washington D.C. 1997.

Joint Publication (JP) 6-0: *Joint Communications Systems*. United States: Chairman, Joint Chiefs of Staff, Washington D.C. 2006.

Joint Publication (JP) 5-0, *Joint Operation Planning*. United States: Chairman, Joint Chiefs of Staff, Washington D.C. 2006.

- Libicki, Martin C. *Defending Cyberspace and Other Metaphors*, National Defense University, Washington, D.C. 1997.
- Naval Network Warfare Command (NETWARCOM) *Strategic Plan 2006-2010 (Version 2.1)*, NETWARCOM, Norfolk. 1 November 2007.  
<http://www.netwarcom.navy.mil/> (Last accessed 16 July 2008).
- Office of Management and Budget (OMB): *Fiscal Year 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, United States: Office of Management and Budget, Washington D.C. 2005.  
<http://www.whitehouse.gov/omb/> (Last accessed 25 August 2008).
- Office of Management and Budget (OMB): *Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, United States Office of Management and Budget, Washington D.C. 2007.  
<http://www.whitehouse.gov/omb/> (Last accessed 25 August 2008).
- Office of Management and Budget (OMB): *Fiscal Year 2007 Report Scorecard of The Federal Information Security Management Act of 2002*, United States: Office of Management and Budget, Washington D.C. 2007.  
<http://results.gov/agenda/scorecard.html> (Last accessed 25 August 2008)
- OMB Circular A-130, *Management of Federal Information Resources*, United States: Office of Management and Budget, Washington, D.C. 2000.  
<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html> (Last accessed 09 August 2008).
- OMB Circular A-130 Appendix III: *Security of Federal Automated Information Resources*, United States: Office of Management and Budget (OMB), Washington, DC, 2000.
- President of the United States, *The National Strategy to Secure Cyberspace*. United States: The White House, Washington D.C. 2003.  
[http://www.dhs.gov/xlibrary/assets/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf) (Last accessed 05 September 2008).
- Randazzo, Marissa and Dawn Cappelli, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, National Threat Assessment Center, United States Secret Service and CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh PA, 2005.  
<http://www.sei.cmu.edu/publications/documents/04.reports/04tr021/04tr021.html> (Last accessed 22 August 2008).

- Richardson, Robert. *2007 CSI Computer Crime and Security Survey, The 12th Annual Computer Crime and Security Survey*, United States: Department of Justice, Washington D.C. 2005.  
[http://www.gocsi.com/forms/csi\\_survey.jhtml](http://www.gocsi.com/forms/csi_survey.jhtml) (Last accessed 12 August 2008).
- Secretary of the Navy, *SECNAV M-5239.1: Information Assurance Manual*, United States: Department of the Navy, Washington D.C. 2005.  
[www.fas.org/irp/doddir/navy/secnavinst/m5239\\_1.pdf](http://www.fas.org/irp/doddir/navy/secnavinst/m5239_1.pdf) (Last accessed 02 September 2008).
- Starling, H. Denby, VADM, NETWARCOM brief Presented to Naval Postgraduate School, United States: Department of Navy, Norfolk, VA, 1 April 2008.
- The Computer Security Act of 1987.  
[http://en.wikipedia.org/wiki/Computer\\_Security\\_Act\\_of\\_1987](http://en.wikipedia.org/wiki/Computer_Security_Act_of_1987) (Last accessed 15 August 2008).
- United States Army Information Assurance Training Center website:  
<https://ia.gordon.army.mil> (Last accessed 02 September 2008).
- United States Congress (107<sup>th</sup> Congress), H.R. 2458 Title III of the E-Government Act of 2002, *Information Security*, 44 U.S.C. § 3541, 2002.  
<http://uscode.house.gov/download/pls/44C35.txt> (Last accessed 20 August 2008).
- United States Marine Corps (USMC) IA Headquarters website:  
<http://www.quantico.usmc.mil/activities/?Section=IA> (Last accessed 02 September 2008).
- Van Wyk, Kenneth, *Build Security In: Training and Awareness*, Carnegie Mellon University, Pittsburgh, PA (Sponsored by Department of Homeland Security National Cyber Security Division), 2008.  
<https://buildsecurityin.us-cert.gov/daisy/bsi/home.html> (Last accessed 30 August 2008).
- Wilshusen, Gregory, *GAO-08-496T: Information Security Issues (FISMA Analysis)*, United States: US Government Accountability Office, Washington D.C. February 2008. [Http://www.gao.gov/new.items/d08496t.pdf](http://www.gao.gov/new.items/d08496t.pdf) (Last accessed 31 August 2008).
- Woody, Carol and Larry Clinton, *Common Sense Guide to Cyber Security for Small Businesses, Recommended Actions for Information Security*. 1st ed., Carnegie Mellon University and Internet Security Alliance, 2004, 8 Mar. 2007  
[http://www.us-cert.gov/reading\\_room/CSG-small-business.pdf](http://www.us-cert.gov/reading_room/CSG-small-business.pdf) (Last accessed 31 August 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dr. Dan Boger  
Naval Postgraduate School  
Monterey, California
4. Terry E. Smith  
Naval Postgraduate School  
Monterey, California
5. Ray Elliott  
Naval Postgraduate School  
Monterey, California
6. Michael A. Herrera  
Naval Postgraduate School  
Monterey, California